GAO Highlights

Highlights of GAO-16-265, a report to congressional requesters

March 2016

HEALTHCARE.GOV

Actions Needed to Enhance Information Security and Privacy Controls

Why GAO Did This Study

The Patient Protection and Affordable Care Act required the establishment of health insurance marketplaces in each state to allow consumers to compare, select, and purchase health insurance plans. States establishing their own marketplaces are responsible for securing the supporting information systems to protect sensitive personal information they contain. CMS is responsible for overseeing states' efforts, as well as securing federal systems to which marketplaces connect, including its data hub.

GAO was asked to review security issues related to the data hub, and CMS oversight of state-based marketplaces. Its objectives were to (1) describe security and privacy incidents reported for Healthcare.gov and related systems, (2) assess the effectiveness of security controls for the data hub, and (3) assess CMS oversight of state-based marketplaces and the security of selected state-based marketplaces. GAO reviewed incident data, analyzed networks and controls, reviewed policies and procedures, and interviewed CMS and marketplace officials. This is a public version of a limited official use only report that GAO issued in March 2016. Sensitive information on technical issues has been omitted from this version.

What GAO Recommends

GAO is recommending that CMS define procedures for overseeing the security of state-based marketplaces and require continuous monitoring of state marketplace security controls. HHS concurred with GAO's recommendations.

View GAO-16-265. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

The Centers for Medicare & Medicaid Services (CMS) reported 316 security-related incidents, between October 2013 and March 2015, affecting Healthcare.gov—the web portal for the federal health insurance marketplace—and its supporting systems. According to GAO's review of CMS records for this period, the majority of these incidents involved such things as electronic probing of CMS systems by potential attackers, which did not lead to compromise of any systems, or the physical or electronic mailing of sensitive information to an incorrect recipient. None of the incidents included evidence that an outside attacker had successfully compromised sensitive data, such as personally identifiable information.

Consistent with federal guidance, CMS has taken steps to protect the security and privacy of data processed and maintained by the systems and connections supporting Healthcare.gov, including the Federal Data Services Hub (data hub). The data hub is a portal for exchanging information between the federal marketplace and CMS's external partners. To protect these systems, CMS assigned responsibilities to appropriate officials and documented information security policies and procedures.

However, GAO identified weaknesses in technical controls protecting the data flowing through the data hub. These included

- insufficiently restricted administrator privileges for data hub systems,
- inconsistent application of security patches, and
- insecure configuration of an administrative network.

GAO also identified additional weaknesses in technical controls that could place sensitive information at risk of unauthorized disclosure, modification, or loss. In a separate report, with limited distribution, GAO recommended 27 actions to mitigate the identified weaknesses.

In addition, while CMS has taken steps to oversee the security and privacy of data processed and maintained by state-based marketplaces, improvements are needed. For example, CMS assigned roles and responsibilities to various oversight entities, met regularly with state officials, and developed a reporting tool to monitor performance. However, it has not defined specific oversight procedures, such as the timing for when each activity should occur, or what follow-up corrective actions should be performed if deficiencies are identified. Further, CMS does not require sufficiently frequent monitoring of the effectiveness of security controls for state-based marketplaces, only requiring testing once every 3 years.

GAO identified significant weaknesses in the controls at three selected state-based marketplaces. These included insufficient encryption and inadequately configured firewalls, among others. In September 2015, GAO reported these results to the three states, which generally agreed and have plans in place to address the weaknesses. Without well-defined oversight procedures and more frequent monitoring of security controls, CMS has less assurance that state-based marketplaces are adequately protected against risks to the sensitive data they collect, process, and maintain.