September 2014

HEALTHCARE.GOV

Actions Needed to Address Weaknesses in Information Security and Privacy Controls

GAO Highlights

Highlights of GAO-14-730, a report to congressional requesters

Why GAO Did This Study

PPACA required the establishment of health insurance marketplaces to assist individuals in obtaining private health insurance coverage. The Department of Health and Human Services' CMS is responsible for overseeing the establishment of these marketplaces, including creating the website for obtaining coverage. The marketplaces became operational on October 1, 2013. As requested, this report examines the security and privacy of the Healthcare.gov website.

GAO (1) describes the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assesses the effectiveness of the programs and controls implemented by CMS to protect the security and privacy of the information and IT systems used to support Healthcare.gov. GAO compared the implementation of controls over Healthcare.gov's supporting systems with privacy and security requirements and guidelines. This is a public version of a limited official use only report that GAO issued in September 2014. Certain information on technical issues has been omitted from this version.

What GAO Recommends

GAO is making six recommendations to implement security and privacy management controls to help ensure that the systems and information related to Healthcare.gov are protected. HHS concurred but disagreed in part with GAO's assessment of the facts for three recommendations. However, GAO continues to believe its recommendations are valid, as discussed in the report.

View GAO-14-730. 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

Many systems and entities exchange information to carry out functions that support individuals' ability to use Healthcare.gov to compare, select, and enroll in private health insurance plans participating in the federal marketplaces, as required by the Patient Protection and Affordable Care Act (PPACA). The Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key federal systems supporting Healthcare.gov, including the Federally Facilitated Marketplace (FFM) system, which contains several modules that perform key functions related to health plan enrollment, and the Federal Data Services Hub (data hub), which provides connectivity between the FFM and other state and federal systems. CMS is also responsible for overseeing state-based marketplaces, which vary in the extent to which they exchange information with CMS. Other federal agencies, including the Department of Defense, Department of Homeland Security, Internal Revenue Service, Office of Personnel Management, Peace Corps, Social Security Administration, and the Department of Veterans Affairs also play key roles in maintaining systems that connect with CMS systems to perform eligibility-checking functions. Finally, a number of commercial entities, including CMS contractors, participating issuers of qualified health plans, agents, and others also connect to the network of systems that support enrollment in Healthcare.gov.

While CMS has taken steps to protect the security and privacy of data processed and maintained by the complex set of systems and interconnections that support Healthcare.gov, weaknesses remain both in the processes used for managing information security and privacy as well as the technical implementation of IT security controls. CMS took many steps to protect security and privacy, including developing required security program policies and procedures, establishing interconnection security agreements with its federal and commercial partners, and instituting required privacy protections. However, Healthcare.gov had weaknesses when it was first deployed, including incomplete security plans and privacy documentation, incomplete security tests, and the lack of an alternate processing site to avoid major service disruptions. While CMS has taken steps to address some of these weaknesses, it has not yet fully mitigated all of them. In addition, GAO identified weaknesses in the technical controls protecting the confidentiality, integrity, and availability of the FFM. Specifically, CMS had not: always required or enforced strong password controls, adequately restricted access to the Internet, consistently implemented software patches, and properly configured an administrative network. An important reason that all of these weaknesses occurred and some remain is that CMS did not and has not yet ensured a shared understanding of how security was implemented for the FFM among all entities involved in its development. Until these weaknesses are fully addressed, increased and unnecessary risks remain of unauthorized access, disclosure, or modification of the information collected and maintained by Healthcare.gov and related systems, and the disruption of service provided by the systems.