GAO Highlights

Highlights of GAO-14-871T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

PPACA requires the establishment of health insurance marketplaces in each state to assist individuals in comparing, selecting, and enrolling in health plans offered by participating issuers. CMS is responsible for overseeing these marketplaces, including establishing a federally facilitated marketplace in states that do not establish their own. These marketplaces are supported by an array of IT systems, including Healthcare.gov, the website that serves as the consumer portal to the marketplace.

This statement is based on two September 2014 reports examining the security and privacy of the Healthcare.gov website and related systems. The specific objectives of this work were to (1) describe the planned exchanges of information between the Healthcare.gov website and other organizations and (2) assess the effectiveness of programs and controls implemented by CMS to protect the security and privacy of the information and IT systems supporting Healthcare.gov.

What GAO Recommends

In its September 2014 reports GAO made 6 recommendations to HHS to implement security and privacy controls to enhance the protection of systems and information related to Healthcare.gov. In addition, GAO made 22 recommendations to resolve technical weaknesses in security controls. HHS agreed with 3 of the 6 recommendations, partially agreed with 3, agreed with all 22 technical recommendations, and described plans to implement them.

View GAO-14-871T. 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.

September 18, 2014

HEALTHCARE.GOV

Information Security and Privacy Controls Should Be Enhanced to Address Weaknesses

What GAO Found

Enrollment through Healthcare.gov is supported by the exchange of information among many systems and entities. The Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS) has overall responsibility for key information technology (IT) systems supporting Healthcare.gov. These include, among others, the Federally Facilitated Marketplace (FFM) system, which facilitates eligibility and enrollment, plan management, and financial management, and the Federal Data Services Hub, which acts as the single portal for exchanging information between the FFM and other systems or external partners. CMS relies on a variety of federal, state, and private-sector entities to support Healthcare.gov activities. For example, it exchanges information with the Department of Defense, Department of Homeland Security, Department of Veterans Affairs, Internal Revenue Service, Office of Personnel Management, Peace Corps, and the Social Security Administration to help determine applicants' eligibility for healthcare coverage and/or financial assistance. Healthcare.gov-related systems are also accessed and used by CMS contractors, issuers of qualified health plans, state agencies, and others.

While CMS has security and privacy-related protections in place for Healthcare.gov and related systems, weaknesses exist that put these systems and the sensitive personal information they contain at risk. Specifically, CMS established security-related policies and procedures for Healthcare.gov, including interconnection security agreements with the federal agencies with which it exchanges information. It also instituted certain required privacy protections, such as notifying the public of the types of information that will be maintained in the system. However, weaknesses remained in the security and privacy protections applied to Healthcare.gov and its supporting systems. For example, CMS did not

- ensure system security plans contained all required information, which makes it harder for officials to assess the risks involved in operating those systems;
- analyze privacy risks associated with Healthcare.gov systems or identify mitigating controls;
- perform comprehensive security testing of the FFM system, reducing assurance that security controls are operating as intended; and
- fully establish an alternate processing site for Healthcare.gov systems to ensure that they could be recovered in the event of a disruption or disaster.

In addition, a number of weaknesses in specific technical security controls jeopardized Healthcare.gov-related systems. These included certain systems supporting the FFM not being restricted from accessing the Internet and inconsistent implementation of security patches, among others.

An underlying reason for many of these weaknesses is that CMS did not establish a shared understanding of security roles and responsibilities with all parties involved in securing Healthcare.gov systems. Until these weaknesses are addressed, the systems and the information they contain remain at increased risk of unauthorized use, disclosure, modification, or loss.