September 2008

HEALTH INFORMATION TECHNOLOGY

HHS Has Taken Important Steps to Address Privacy Principles and Challenges, Although More Work Remains

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-1138, a report to the Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Although advances in information technology (IT) can improve the quality and other aspects of health care, the electronic storage and exchange of personal health information introduces risks to the privacy of that information. In January 2007, GAO reported on the status of efforts by the Department of Health and Human Services (HHS) to ensure the privacy of personal health information exchanged within a nationwide health information network. GAO recommended that HHS define and implement an overall privacy approach for protecting that information. For this report, GAO was asked to provide an update on HHS's efforts to address the January 2007 recommendation. To do so, GAO analyzed relevant HHS documents that described the department's privacy-related health IT activities.

What GAO Recommends

GAO recommends that HHS include in its overall privacy approach a process for ensuring that key privacy principles and challenges are completely and adequately addressed. In written comments on a draft of this report, HHS generally agreed with the information discussed in the report.

To view the full product, including the scope and methodology, click on GAO-08-1138. For more information, contact Valerie C. Melvin, (202) 512-6304 or melvinv@gao.gov.

What GAO Found

Since GAO's January 2007 report on protecting the privacy of electronic personal health information, the department has taken steps to address the recommendation that it develop an overall privacy approach that included (1) identifying milestones and assigning responsibility for integrating the outcomes of its privacy-related initiatives, (2) ensuring that key privacy principles are fully addressed, and (3) addressing key challenges associated with the nationwide exchange of health information. In this regard, the department has fulfilled the first part of GAO's recommendation, and it has taken important steps in addressing the two other parts. The HHS Office of the National Coordinator for Health IT has continued to develop and implement health IT initiatives related to nationwide health information exchange. These initiatives include activities that are intended to address key privacy principles and challenges. For example:

- The Healthcare Information Technology Standards Panel defined standards for implementing security features in systems that process personal health information.
- The Certification Commission for Healthcare Information Technology defined certification criteria that include privacy protections for both outpatient and inpatient electronic health records.
- Initiatives aimed at the state level have convened stakeholders to identify and propose solutions for addressing challenges faced by health information exchange organizations in protecting the privacy of electronic health information.

In addition, the office has identified milestones and the entity responsible for integrating the outcomes of its privacy-related initiatives, as recommended. Further, the Secretary released a federal health IT strategic plan in June 2008 that includes privacy and security objectives along with strategies and target dates for achieving them.

Nevertheless, while these steps contribute to an overall privacy approach, they have fallen short of fully implementing GAO's recommendation. In particular, HHS's privacy approach does not include a defined process for assessing and prioritizing the many privacy-related initiatives to ensure that key privacy principles and challenges will be fully and adequately addressed. As a result, stakeholders may lack the overall policies and guidance needed to assist them in their efforts to ensure that privacy protection measures are consistently built into health IT programs and applications. Moreover, the department may miss an opportunity to establish the high degree of public confidence and trust needed to help ensure the success of a nationwide health information network.