January 2007

HEALTH INFORMATION TECHNOLOGY

Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-238, a report to congressional requesters

Why GAO Did This Study

The expanding implementation of health information technology (IT) and electronic health information exchange networks raises concerns regarding the extent to which the privacy of individuals' electronic health information is protected. In April 2004, President Bush called for the Department of Health and Human Services (HHS) to develop and implement a strategic plan to guide the nationwide implementation of health IT. The plan is to recommend methods to ensure the privacy of electronic health information.

GAO was asked to describe HHS's efforts to ensure privacy as part of its national strategy and to identify challenges associated with protecting electronic personal health information. To do this, GAO assessed relevant HHS privacy-related initiatives and analyzed information from health information organizations.

What GAO Recommends

GAO recommends that HHS define and implement an overall privacy approach that identifies milestones for integrating the outcomes of its initiatives, ensures that key privacy principles are fully addressed, and addresses challenges associated with the nationwide exchange of health information. In its comments, HHS disagreed and stated that it has established a comprehensive privacy approach. However, GAO believes that an overall approach for integrating HHS's initiatives has not been fully defined and implemented.

www.gao.gov/cgi-bin/getrpt?GAO-07-238.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz, (202) 512-6240 or koontzl@gao.gov.

What GAO Found

HHS and its Office of the National Coordinator for Health IT have initiated actions to identify solutions for protecting personal health information through several contracts and with two health information advisory committees. For example, in late 2005, HHS awarded several health IT contracts that include requirements for addressing the privacy of personal health information exchanged within a nationwide health information exchange network. Its privacy and security solutions contractor is to assess the organization-level privacy- and security-related policies, practices, laws, and regulations that affect interoperable health information exchange. Additionally, in June 2006, the National Committee on Vital and Health Statistics made recommendations to the Secretary of HHS on protecting the privacy of personal health information within a nationwide health information network, and in August 2006, the American Health Information Community convened a work group to address privacy and security policy issues for nationwide health information exchange. While these activities are intended to address aspects of key principles for protecting the privacy of health information, HHS is in the early stages of its efforts and has therefore not yet defined an overall approach for integrating its various privacy-related initiatives and addressing key privacy principles, nor has it defined milestones for integrating the results of these activities.

GAO identified key challenges associated with protecting electronic personal health information in four areas (see table).

Challenges to Exchanging Electronic Health Information

Area	
Understanding and resolving legal and policy issues	• Resolving uncertainties regarding the extent of federal privacy protection required of various organizations • Understanding and resolving data sharing issues introduced by varying state privacy laws and organization-level practices • Reaching agreements on differing interpretations and applications of HIPAA privacy and security rules • Determining liability and enforcing sanctions in case of breaches of confidentiality
Ensuring appropriate disclosure	• Determining the minimum data necessary that can be disclosed in order for requesters to accomplish their intended purposes • Determining the best way to allow patients to participate in and consent to electronic health information exchange • Educating consumers about the extent to which their consent to use and disclose health information applies
Ensuring individuals' rights to request access and amendments to health information	• Ensuring that individuals understand that they have rights to access and amend their own health information • Ensuring that individuals' amendments are properly made and tracked across multiple locations
Implementing adequate security measures for protecting health information	• Determining and implementing adequate techniques for authenticating requesters of health information • Implementing proper access controls and maintaining adequate audit trails for monitoring access to health data • Protecting data stored on portable devices and transmitted between business partners

Source: GAO analysis of information provided by state-level health information exchange organizations, federal health care providers, and health IT professional associations.