August 2016

ELECTRONIC HEALTH INFORMATION

HHS Needs to Strengthen Security and Privacy Guidance and Oversight

GAO Highlights

Highlights of GAO-16-771, a report to the Committee on Health, Education, Labor, and Pensions, U.S. Senate

Why GAO Did This Study

As a digital version of a patient's medical record or chart, an EHR can make pertinent health information more readily available and usable for providers and patients. However, recent data breaches highlight the need to ensure the security and privacy of these records. HHS has primary responsibility for setting standards for protecting electronic health information and for enforcing compliance with these standards.

GAO was asked to review the current health information cybersecurity infrastructure. The specific objectives were to (1) describe expected benefits of and cyber threats to electronic health information, (2) determine the extent to which HHS security and privacy guidance for EHRs are consistent with federal cybersecurity guidance, and (3) assess the extent to which HHS oversees these requirements. To address these objectives, GAO reviewed relevant reports, federal guidance, and HHS documentation and interviewed subject matter experts and agency officials.

What GAO Recommends

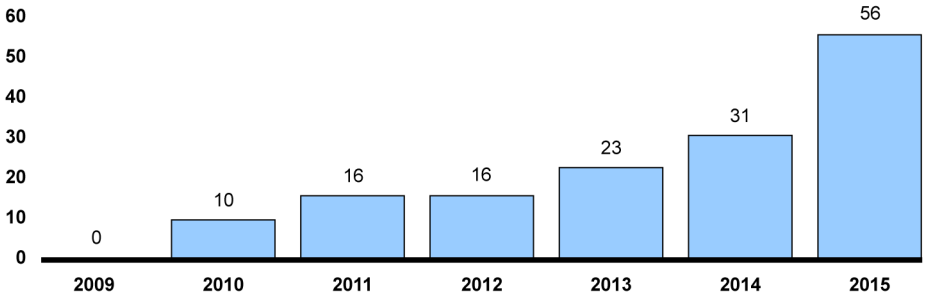
GAO is making five recommendations, including that HHS update its guidance for protecting electronic health information to address key security elements, improve technical assistance it provides to covered entities, follow up on corrective actions, and establish metrics for gauging the effectiveness of its audit program. HHS generally concurred with the recommendations and stated it would take actions to implement them.

View GAO-16-771. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The use of electronic health information can allow providers to more efficiently share information and give patients easier access to their health information, among other benefits. Nonetheless, systems storing and transmitting health information in electronic form are vulnerable to cyber-based threats. The resulting breaches—involving over 113 million records in 2015—can have serious adverse impacts such as identity theft, fraud, and disruption of health care services, and their number has increased steadily in recent years, from 0 in 2009 to 56 in 2015 (see figure).

Number of Reported Hacking and Information Technology Breaches Affecting Health Care Records of 500 or More Individuals



Source: GAO analysis of Department of Health and Human Services data. | GAO-16-771

The Department of Health and Human Services (HHS) has established guidance for covered entities, such as health plans and care providers, for use in their efforts to comply with HIPAA requirements regarding the privacy and security of protected health information, but it does not address all elements called for by other federal cybersecurity guidance. Specifically, HHS's guidance does not address how covered entities should tailor their implementations of key security controls identified by the National Institute of Standards and Technology to their specific needs. Such controls include developing risk responses, among others. Further, covered entities and business associates have been challenged to comply with HHS requirements for risk assessment and management. Without more comprehensive guidance, covered entities may not be adequately protecting electronic health information from compromise.

HHS has established an oversight program for compliance with privacy and security regulations, but actions did not always fully verify that the regulations were implemented. Specifically, HHS's Office of Civil Rights investigates complaints of security or privacy violations, almost 18,000 of which were received in 2014. It also has established an audit program for covered entities' security and privacy programs. However, for some of its investigations it provided technical assistance that was not pertinent to identified problems, and in other cases it did not always follow up to ensure that agreed-upon corrective actions were taken once investigative cases were closed. Further, the office has not yet established benchmarks to assess the effectiveness of its audit program. These weaknesses result in less assurance that loss or misuse of health information is being adequately addressed.