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.