June 2012

PRESCRIPTION DRUG DATA

HHS Has Issued Health Privacy and Security Regulations but Needs to Improve Guidance and Oversight

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-605, a report to congressional committees

Why GAO Did This Study

Prescribing medications and filling those prescriptions increasingly relies on the electronic collection of individuals' health information and its exchange among health care providers, pharmacies, and other parties. While this can enhance efficiency and accuracy, it also raises privacy and security concerns. Federal law establishes the authority for the Secretary of HHS to develop standards for protecting individuals' health information (which includes Medicare beneficiaries) and to ensure that covered entities (such as health care providers and pharmacies) and their business associates comply with these requirements.

The Medicare Improvements for Patients and Providers Act of 2008 required GAO to report on prescription drug use data protections. GAO's specific objective for this review was to determine the extent to which HHS has established a framework to ensure the privacy and security of Medicare beneficiaries' protected health information when data on prescription drug use are used for purposes other than direct clinical care. To do this, GAO reviewed HHS policies and other related documentation and interviewed agency officials.

What GAO Recommends

GAO recommends that HHS issue de-identification guidance and establish a plan for a sustained audit capability. HHS generally agreed with both recommendations but disagreed with GAO's assessment of the impacts of the missing guidance and lack of an audit capability. In finalizing its report, GAO qualified these statements as appropriate.

View GAO-12-605. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

While the Department of Health and Human Services (HHS) has established a framework for protecting the privacy and security of Medicare beneficiaries' prescription drug use information when used for purposes other than direct clinical care through its issuance of regulations, outreach, and enforcement activities, it has not issued all required guidance or fully implemented required oversight capabilities. HHS has issued regulations including the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules to safeguard protected health information from unauthorized use and disclosure. Through its Office for Civil Rights (OCR), HHS has undertaken a variety of outreach and educational efforts to inform members of the public and covered entities about the uses of protected health information. Specifically, OCR has made available on its website guidance and other materials informing the public about the uses to which their personal information may be put and the protections afforded to that information by federal laws. It has also made available guidance to covered entities and their business associates that is intended to promote compliance with the HIPAA Privacy and Security Rules.

However, HHS has not issued required implementation guidance to assist entities in de-identifying personal health information including when it is used for purposes other than directly providing clinical care to an individual. This means ensuring that data cannot be linked to a particular individual, either by removing certain unique identifiers or by applying a statistical method to ensure that the risk is very small that an individual could be identified. According to OCR officials, the completion of the guidance, required by statute to be issued by February 2010, was delayed due to competing priorities for resources and internal reviews. Until the guidance is issued, increased risk exists that covered entities are not properly implementing the standards set forth by federal regulations for de-identifying protected health information.

Additionally, in enforcing compliance with the HIPAA Privacy and Security Rules, OCR has established an investigations process for responding to reported violations of the rules. Specifically, the office annually receives thousands of complaints from individuals and notices of data breaches from covered entities, and initiates investigations as appropriate. If it finds that a violation has occurred, the office can require covered entities to take corrective action and pay fines and penalties.

HHS was also required by law to implement periodic compliance audits of covered entities' compliance with HHS privacy and security requirements; however, while it has initiated a pilot program for conducting such audits, it does not have plans for establishing a sustained audit capability. According to OCR officials, the office has completed 20 audits and plans to complete 95 more by the end of December 2012, but it has not established plans for continuing the audit program after the completion of the pilots or for auditing covered entities' business associates. Without a plan for establishing an ongoing audit capability, OCR will have limited assurance that covered entities and business associates are complying with requirements for protecting the privacy and security of individuals' personal health information.