GAO Highlights

Highlights of GAO-18-210, a report to congressional requesters

March 2018

# ELECTRONIC HEALTH INFORMATION

## CMS Oversight of Medicare Beneficiary Data Security Needs Improvement

## Why GAO Did This Study

Recent data breaches have highlighted the importance of ensuring the security of health information, including Medicare beneficiary data. Such data are created, stored, and used by a wide variety of entities, such as health care providers, insurance companies, financial institutions, researchers, and others.

GAO was asked to conduct a study of CMS efforts to protect Medicare beneficiary data accessed by external entities. GAO's objectives were to (1) identify the major external entities that collect, store, and process Medicare fee-for-service beneficiary data; (2) determine whether requirements for the protection of Medicare beneficiary data align with federal guidance; and (3) assess CMS oversight of the implementation of those requirements. GAO analyzed information about how external entities access data, reviewed CMS documentation on who they share data with, compared federal standards with CMS security requirements for external entities, and analyzed results of independent security reviews. GAO also interviewed CMS officials about their oversight activities.

## What GAO Recommends

GAO recommends that CMS develop additional guidance for researchers on implementing security controls required by CMS, consistently track results of independent assessments, and provide oversight of researchers and qualified entities. CMS concurred with GAO's three recommendations and described actions it has planned or taken to address them.

View GAO-18-210. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

## What GAO Found

The Centers for Medicare and Medicaid Services (CMS) shares Medicare beneficiary data with three major types of external entities: (1) Medicare Administrative Contractors (MAC) that perform processing and distribution functions that support the payment of Medicare benefits; (2) research organizations (researchers) that use Medicare beneficiary data to study how health care services are provided to beneficiaries; and (3) qualified public or private entities that use claims data to evaluate the performance of Medicare service providers and equipment suppliers.

CMS has developed requirements for implementing security controls that align with federal guidance for two of the three types of external entities that access Medicare beneficiary data. While CMS has developed guidance for MACs and qualified entities, it has not developed equivalent guidance for researchers. Researchers must adhere to broad governmentwide standards, but are not given guidance on which specific controls to implement. According to CMS, the lack of specific guidance gives the researchers more flexibility to independently assess their security risks and determine which controls are appropriate to implement; however, without providing comprehensive, risk-based security guidance to researchers, CMS increases the risk that external entities possessing agency data may not have applied security controls that meet CMS standards.

Additionally, CMS has established an oversight program for the security of MAC data, but has not established a corresponding program to oversee security implementation by researchers and qualified entities. Without effective oversight measures in place for researchers and qualified entities, CMS cannot fully ensure that the security of Medicare beneficiary data is being adequately protected. Regarding MACs, although they are subject to two types of independent annual assessments, which have regularly identified weaknesses in their implementation of security controls, the weaknesses that have been assessed as low-risk have not been consistently tracked in the CMS finding tracking system. Without more consistent tracking of these low-risk weaknesses, it may be difficult for CMS to determine if all weaknesses are being addressed in a timely manner. Examples of categories of recurring weaknesses that have been identified during annual assessments are listed in the table.

**Table: Key Recurring Categories of Weaknesses Identified in Annual Assessments of Medicare Administrative Contractors**

| Category | Significance |
|---|---|
| Configuration management | Ensures that software updates are timely, appropriate, and do not introduce new security weaknesses. |
| System security plans | Allows assessors to review a system's security strategy and determine whether security has been implemented as intended. |
| System inventories | Ensures that organizations have a complete and up-to-date inventory of hardware and software components as a basis for effective configuration management. |

Source: GAO analysis of annual MAC assessments.