November 2024 | A-18-21-08014

The Office for Civil Rights Should Enhance Its HIPAA Audit Program to Enforce HIPAA Requirements and Improve the Protection of Electronic Protected Health Information

Why OIG Did This Audit

- The increase in the number of successful cyberattacks against health care organizations' information technology (IT) systems raises the question of whether OCR's audits, guidance, and enforcement activities for ensuring the protection of electronic protected health information (ePHI) have been effective. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required HHS to develop national standards for the use and dissemination of health care information, including standards to protect ePHI.
- In this audit, OIG evaluated OCR's program for performing periodic HIPAA audits, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act.

What OIG Found

OCR fulfilled its requirement under the HITECH Act to perform periodic HIPAA audits. However:

- OCR's HIPAA audit implementation was too narrowly scoped to effectively assess ePHI protections and demonstrate a reduction of risks within the health care sector. Specifically:
    - OCR's audits consisted of assessing only 8 of 180 HIPAA Rules requirements; and
    - only 2 of those 8 requirements were related to Security Rule administrative safeguards and none were related to physical and technical security safeguards.
- OCR oversight of its HIPAA audit program was not effective at improving cybersecurity protections at covered entities and business associates.

What OIG Recommends

We made a series of recommendations to OCR to enhance its HIPAA audit program, including that it expand the scope of its HIPAA audits to assess compliance with physical and technical safeguards from the HIPAA Security Rule, document and implement standards and guidance for ensuring that deficiencies identified during the HIPAA audits are corrected in a timely manner, and define metrics for monitoring the effectiveness of OCR's HIPAA audits at improving audited covered entities and business associates' protections over ePHI and periodically review whether these metrics should be refined. The full recommendations are in the report.

OCR did not concur with one recommendation but concurred with our three other recommendations and detailed steps it has taken and plans to take in response.