HHS Needs to Improve Communications for Breach Reporting

What GAO Found

Since 2015, the Department of Health and Human Services (HHS) has seen an increase in reported breaches while the number of affected individuals has varied each year from approximately 5 to 113 million. Such breaches of health information involve the unauthorized (intentional or unintentional) exposure, disclosure, or loss of an individual’s identifiable health information. The figure shows the number of breaches reported by various covered entities from 2015 through 2021.

![Figure: The Number of Breaches Involving Unsecured Protected Health Information (PHI) from 2015 to 2021](image)

*Note: Business associates are entities that perform certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Health care clearinghouses are entities that process nonstandard data elements of health information they receive from another entity into standard data elements or vice versa.

The HHS Office for Civil Rights (OCR), the unit responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA) standards, has taken steps to establish a process on whether entities implemented recognized security practices. A law enacted in January 2021 required HHS, as part of its enforcement activities, to consider whether covered entities had implemented such practices. In response, OCR established standard operating procedures for its investigators, published a request for information to seek public comments on implementation of security practices, and is conducting outreach to the health care sector. OCR expects to finalize the process no later than the summer of 2022.

OCR is charged with implementing and enforcing the HIPAA Privacy, Security and Breach Notification Rules, including the development and management of the breach reporting process. However, OCR does not have a method for covered entities to provide feedback on the breach reporting process, nor did the office indicate that it had plans to develop one. Without a clear mechanism to provide feedback to OCR, covered entities and business associates can face challenges during the breach reporting process. Further, soliciting feedback on the breach reporting process could help OCR improve aspects of the process.

What GAO Recommends

GAO is making one recommendation to HHS to establish a feedback mechanism to improve the effectiveness of its breach reporting process. HHS concurred with GAO’s recommendation and described actions it would take to address it.

*View GAO-22-105425. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov or Marisol Cruz Cain at (202) 512-5017 or CruzCainM@gao.gov.*