STRATEGIC MANAGEMENT SERVICES

OIG Reports OCR Weakness in HIPAA Privacy Oversight

Richard P. Kusserow | January 2025

The 2024 Compliance Benchmark Survey found that healthcare providers were many times more likely to have encounters with the Office of Civil Rights (OCR) as a result of a breach in protected health information than with the DOJ, OIG, or a MFCU over any other type of regulatory or legal issue. OCR reported receiving in 2023 a 239% increase in large breaches involving hacking and a 278% increase in ransomware, and that the large breaches reported had affected over 88 million individuals, a 60% increase from the previous year. The OIG conducted a review of OCR oversight of covered entities and issued a report that their work was inadequate in meeting compliance with the Privacy Rule. This included not taking appropriate steps to mitigate cybersecurity risks to healthcare organizations. It noted that OCR was primarily reactive in responding to complaints and not fully implementing the required audit program to proactively assess possible noncompliance from covered entities. They further found that OCR did not adequately hold covered entities and their business associates accountable for known issues with privacy and security. Also included in their report was that OCR did not audit entities on enough benchmarks regarding the security of electronic protected health information (ePHI), having only assessed eight of the 180 standards set out in HIPAA across privacy, security, and health breach notification. Finally, they found that OCR did not perform additional compliance reviews when the office identified concerns with privacy and security practices from a voluntary audit.

The OIG called for OCR to: (a) fully implement a permanent audit program; (b) maintain complete documentation of corrective action; (c) develop an efficient method in its case-tracking system to search for and track covered entities; (d) develop a policy requiring OCR staff to check whether covered entities have been previously investigated; (e) continue to expand outreach and education efforts to covered entities; (f) add more data security benchmarks to its compliance audits; (g) expand the scope of audits to include physical and technical security safeguards; (h) define and document criteria for determining whether a compliance issue identified during a HIPAA audit should result in OCR initiating a compliance review; and (j) periodically review whether these metrics should be refined.

The OCR agreed with most of the recommendations, including auditing covered entities for more physical and technical security safeguards. However, they noted that they had only 60 investigative staff in 2022, an all-time low, while health breach notification complaints reached 51,779 complaints, an all-time high. The OCR also requested Congress to provide additional authority for seeking injunctive relief for noncompliance with the HIPAA rules.

Copyright © 2025 Strategic Management Services, LLC

For more information and advice on this subject contact rkusserow@strategicm.com. You can also keep up-to-date with Strategic Management Services by following us on LinkedIn.

About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.

Copyright © 2025 Strategic Management Services, LLC