Provided by National Insurance Services

LEGAL UPDATE

HHS Announces HIPAA Audit Program Will Resume

The U.S. Department of Health and Human Services (HHS) recently updated its HIPAA enforcement website to announce the start of its 2024-25 audit program. HIPAA is enforced by HHS' Office for Civil Rights (OCR). According to OCR, the 2024-25 HIPAA audits will review **50 covered entities' and business associates'** (collectively called regulated entities) compliance with selected provisions of the **HIPAA Security Rule** most relevant to hacking and ransomware attacks.

This is a significant compliance step for OCR, which has not utilized its HIPAA audit program since 2016-17 due to a lack of financial resources. HIPAA audits are primarily a compliance improvement activity; however, if an audit reveals a serious compliance issue, OCR may initiate a compliance review of the regulated entity to investigate.

NIS
National Insurance Services

HIGHLIGHTS

- HHS has announced that its HIPAA audit program will resume.
- Fifty covered entities and business associates will be selected for an audit.
- The audits will focus on selected provisions of the HIPAA Security Rule most relevant to hacking and ransomware attacks.
- Although HIPAA audits are primarily a compliance improvement activity, HHS may investigate a regulated entity if an audit reveals a serious compliance issue.

HIPAA Security Rule

The HIPAA Security Rule sets a national floor for the protection of individuals' electronic protected health information (ePHI) by covered entities (health plans, health care clearinghouses and most health care providers) and their business associates. These standards require regulated entities to analyze the risks and vulnerabilities of the confidentiality, integrity and availability of their ePHI. The risk assessment process helps regulated entities implement reasonable and appropriate administrative, physical and technical safeguards to protect their ePHI.

HIPAA Audit Program

HHS is required to periodically audit regulated entities for compliance with the requirements of HIPAA's Privacy, Security and Breach Notification Rules. OCR last conducted HIPAA audits in 2016-17, when it audited 166 covered entities and 41 business associates.

In a report from Nov. 25, 2024, HHS' Office of Inspector General (OIG) concluded that OCR's HIPAA audit program was not effective at improving cybersecurity protections at regulated entities. OIG made several recommendations for OCR to enhance its HIPAA audit program, including expanding the scope of the audits to assess compliance with the Security Rule's physical and technical safeguards.

In December 2024, OCR announced that HIPAA audits would resume. These audits will focus on compliance provisions of the HIPAA Security Rule that are most related to cybersecurity. OCR will publish an industry report summarizing its findings after the 2024-25 HIPAA audits are completed.

Employers with self-insured health plans and employers with fully insured health plans that have access to ePHI should periodically review their compliance with the HIPAA Security Rule. This review should include ensuring their risk analysis is up to date and they have implemented the appropriate administrative, physical and technical safeguards for ePHI.