Published on *The National Law Review* https://natlawreview.com

OCR Reaches Settlement with Health Care Network Health Over HIPAA Violations Stemming from Phishing Attack

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On April 23, 2025, the Department of Health and Human Services' Office for Civil Rights ("OCR") announced a HIPAA enforcement action against PIH Health, Inc. ("PIH"), a California-based health care network, following a phishing attack that exposed patients' electronic protected health information ("ePHI"). The settlement highlights OCR's continued focus on ensuring that covered entities implement robust security programs capable of identifying and mitigating threats to ePHI.

The investigation stemmed from a breach report submitted by PIH in January 2020, which disclosed that in June 2019, a phishing attack had compromised the email accounts of 45 employees. The attack resulted in the unauthorized disclosure of unsecured ePHI belonging to 189,763 individuals, including names, addresses, dates of birth, driver's license numbers, Social Security numbers, medical diagnoses, lab results, medications, treatment and claims information, and financial data.

OCR's investigation uncovered multiple potential violations of the HIPAA Privacy, Security and Breach Notification Rules, including PIH's failure to (1) use or disclose PHI as required by the Privacy Rule, (2) conduct an accurate and thorough risk analysis of security vulnerabilities affecting ePHI, and (3) provide timely breach notification to affected individuals, HHS, and the media.

To resolve the matter, PIH agreed to a $600,000 monetary settlement and to implement a two-year corrective action plan. Under the corrective action plan, PIH is required to conduct a comprehensive HIPAA risk analysis, develop and implement a risk management plan to address identified vulnerabilities, revise and maintain HIPAA-compliant policies and procedures, and provide workforce training on HIPAA requirements for safeguarding PHI.

This enforcement action underscores OCR's expectation that covered entities proactively assess and strengthen their HIPAA compliance programs to address evolving cybersecurity threats such as phishing attacks. It also follows two recent additional settlements announced by OCR involving failures to implement basic safeguards under the HIPAA Security Rule, reinforcing the agency's continued emphasis on holding regulated entities accountable for cybersecurity-related compliance lapses.

Copyright © 2025, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume XV, Number 122

Source URL:https://natlawreview.com/article/ocr-reaches-settlement-health-care-network-health-over-hipaa-violations-stemming