HHS Investigation of Health Plan Results in $1,300,000 HIPAA Settlement Payment

EBIA Weekly (September 28, 2023)

Resolution Agreement: L.A. Care Health Plan (Aug. 1, 2023); HHS Press Release (Sept. 11, 2023)

Resolution Agreement

Press Release

HHS's Office of Civil Rights (OCR) has announced a resolution agreement with the nation's largest publicly operated health plan that provides benefits through state, federal, and commercial programs, settling potential violations of HIPAA found during two separate incidents. OCR opened the first investigation in January of 2016 based on an online media article about the health plan released in March of 2014, alleging that some members could see other members' PHI when logging onto the payment portal. The second investigation was conducted after the health plan reported to OCR that a breach impacting approximately 1,498 individuals occurred when members received identification cards for other members due to a mailing error.

The resolution agreement requires a $1,300,000 settlement payment and compliance with a corrective action plan (CAP) that will be monitored for three years. Under the CAP, the health plan must: (1) conduct an accurate and thorough risk analysis to determine risks and vulnerabilities to ePHI across the organization; (2) create a risk management plan to reduce the risks and vulnerabilities to ePHI; (3) develop, implement, and distribute policies and procedures; and (4) report to HHS when an evaluation is conducted of environmental and operational changes that affect the security of ePHI or when workforce members fail to comply with HIPAA's rules.

EBIA Comment: Under the HIPAA privacy and security rules, covered entities must implement procedures to verify that a person seeking access to PHI/ePHI is the one claimed, whether the access is through an online portal or mailing. The HHS press release underscores that covered entities are exposed to high penalties if they do not proactively ensure compliance with the HIPAA rules by identifying and mitigating vulnerabilities in processes. It also emphasizes that breaches often reveal systemic noncompliance with the privacy rule, encouraging plan sponsors to affirmatively implement security measures that protect systems and processes. For more information, see EBIA's HIPAA Portability, Privacy & Security manual at XXVIII.H ("Policies and Procedures"), Sections XX.D ("Resolution Agreements"), and XXX.D ("Technical Safeguards").

Contributing Editors: EBIA Staff.