OCR’s Risk Analysis Initiative Going Strong

3/1/2026

On February 19, 2026, the U.S. Department of Health & Human Services, Office for Civil Rights (OCR) issued a press release in which the OCR announced the settlement of its 11th enforcement action in OCR’s Risk Analysis Initiative. The settlement resolved an OCR investigation of an Illinois substance use disorder treatment provider for potential HIPAA violations relating to a successful email phishing attack. Through the attack, the threat actor accessed electronic protected health information (ePHI) through a workforce member’s email account, impacting 1,980 patients.

OCR concluded that the provider had failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI the provider holds, as required by the HIPAA Security Rule. Pursuant to the resolution agreement entered into between the provider and the OCR, the provider agreed to pay a monetary penalty of $103,000, plus enter into a corrective action plan under which the provider must conduct a complete and thorough risk analysis, develop and implement a risk management plan, develop policies and procedures and provide workforce training.

- In its press release, the OCR recommended that HIPAA covered entities and business associates implement steps to mitigate or prevent cyber-threats, including:
- Identify where ePHI is located in the organization, including how ePHI enters, flows through, and leaves the organization’s information systems.
- Periodically conduct, and update as needed, a risk analysis and develop and implement risk management measures to address identified risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
- Ensure audit controls are in place to record and examine information system activity.

- Implement regular review of information system activity.
- Utilize mechanisms to authenticate users seeking access to ePHI.
- Encrypt ePHI in transit and at rest to guard against unauthorized access to ePHI when appropriate.
- Incorporate lessons learned from incidents into the organization's overall security management process.
- Provide workforce members with regular HIPAA training that is specific to the organization and to the workforce members' respective job duties.

Click Here to read the entire March 2026 Healthcare Law Update now!

If you need assistance with your organization's privacy and security program, including assistance with updating your organization's Notice of Privacy Practices, contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com

Authors

The following attorneys contributed to this insight.

Lani M. Dornfeld

CHPC, Member
Healthcare Law

973.403.3136 · 973.618.5536 Fax

ldornfeld@bracheichler.com