OCR Settles 13th Ransomware Enforcement Action

6/1/2025

The U.S. Department of Health & Human Services, Office for Civil Rights (OCR) recently announced the settlement of its 13th ransomware enforcement action and 9th enforcement action in its Risk Analysis Initiative. The settlement resolves an OCR investigation concerning a ransomware breach of a billing and collection service provider (a HIPAA business associate of over 70 HIPAA covered entities) that affected 585,621 individuals.

OCR's investigation revealed that the service provider was the victim of a ransomware attack whereby an unknown actor gained access to electronic protected health information (ePHI) residing on the service provider's network servers and encrypted the network servers. OCR's sole negative finding was that the service provider "failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the ePHI that it holds." Under the Resolution Agreement entered into between the parties, the service provider agreed to pay a civil penalty of $75,000 and implement a corrective action plan OCR will monitor for a period of two years.

In its announcement of the settlement, OCR took the opportunity to recommend to covered entities and business associates that they take 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.

• Integrate risk analysis and risk management into the organization's business processes.

• Ensure that audit controls are in place to record and examine information system activity.

• Implement regular reviews of information system activity.

• Utilize mechanisms to authenticate information to ensure only authorized users are accessing 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 July 2025 Healthcare Law Update now!

For more information or assistance with your organization's privacy and security program, 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