NJ, NY and CT Attorneys General Settle Biotech Company Data Breach for $4.5M

8/30/2024

On August 13, 2024, the New York State Attorney General, Letitia James, announced the settlement reached between the New Jersey, New York and Connecticut Attorneys General and Enzo Biochem, Inc. (Enzo), a biotech company previously offering diagnostic testing services, for its failure to adequately safeguard the personal and private health information of its patients. The Office of the Attorney General (OAG) found that "Enzo had poor data security practices, which led to a ransomware attack that compromised the personal and private information of approximately 2.4 million patients." The $4.5 million penalty will be shared between the three states. In addition to payment of the financial penalty, Enzo agreed to a corrective action plan that includes the requirement to implement a robust information security program.

The settlement came after an investigation by the New York State Attorney General's office following the April 2023 ransomware attack suffered by Enzo. Among the data breached in the attack were names, medical treatment information and Social Security numbers. "In 2023, cyber-attackers were able to access Enzo's networks using two employee login credentials. The OAG later found that those two login credentials were shared between five Enzo employees and one of the login credentials hadn't been changed in the last ten years, putting Enzo at heightened risk of a cyberattack. Once logged in, the attackers installed malicious software on several of Enzo's systems. Enzo was not aware of the attackers' activity until several days later because the company did not have a system or process in place to monitor or provide notice of suspicious activity." As set forth in the Assurance of Discontinuance document signed by the parties, Enzo had performed a security risk assessment in 2021 that revealed vulnerabilities, but failed to implement security recommendations from the assessment. Following the incident, in the summer of 2023, Enzo sold its clinical laboratory testing assets and exited the clinical laboratory business.
Takeaways include:

- Covered entities and their business associates must have in place privacy and security policies and a meaningful security program
- Organizations must perform periodic risk analyses to detect actual and potential risks and vulnerabilities to electronic systems and data
- Results from such assessments must be used to prepare and implement a security management plan, including timeframes for completion of tasks
- Organizations must implement access controls and user authentication procedures
- Organizations must engage in ongoing auditing and monitoring of system activity, and take appropriate and timely action
- Organizations must ensure employees are properly implementing and following security protocols

Organizations that suffer data breaches are at risk of investigation and assessment of penalties not only from the federal DHHS Office for Civil Rights (federal HIPAA enforcement agency), but also from State Attorneys General.

Click Here to read the entire August 2024 Healthcare Law Update now!

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please 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