Warby Parker Pays the Price for Failure to See it Lacked Security Protections



4/1/2025

On February 20, 2025, the OCR announced that it assessed a $1.5 million penalty against eyewear manufacturer and retailer Warby Parker relating to alleged violations of the HIPAA Security Rule. The resolution followed an investigation initiated by the OCR initiated in December 2018 following its receipt of a breach report by Warby Parker. The month earlier, the company became aware of unusual, attempted log-in activity on its website due to a type of cyber attack known as "credential stuffing." Between September and November of that year, unauthorized third parties gained access to Warby Parker customer information by using usernames and passwords obtained from other, unrelated websites that were presumably breached. The breach affected approximately 200,000 individuals. The OCR found evidence of three violations of the HIPAA Security Rule: a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to ePHI in Warby Parker's systems, a failure to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level, and a failure to implement procedures to regularly review records of information system activity.

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

If you need assistance with your 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