Compliance Lessons From Warby Parker's HIPAA Fine

By **Bruce Armon and Bunyad Bhatti** (May 5, 2025)

Bruce Armon

Bunyad Bhatti

New presidential administrations always need to pick and choose their priorities. It will be very interesting and enlightening to see whether and, if so, how the Trump administration will focus resources related to Health Insurance Portability and Accountability Act settlements and civil money penalties.

The Biden administration was active in negotiating HIPAA settlements with covered entities and business associates, and imposing civil money penalties on HIPAA offenders. Several of the Biden HIPAA settlements and civil money penalties have been announced during the early period of the Trump administration, including the civil money penalty detailed below.

The Civil Money Penalty

On Feb. 20, the U.S. Department of Health and Human Services' Office for Civil Rights announced a $1.5 million civil money penalty against Warby Parker Inc. Warby Parker is a manufacturer and online retailer of prescription and nonprescription eyewear. The civil money penalty was finalized on Dec. 11, 2024, but was not announced until Feb. 20.

This civil money penalty is noteworthy because Warby Parker, as a retail-oriented enterprise, illustrates the emerging challenges that consumer-facing brands encounter when expanding into healthcare-adjacent sectors.

As organizations increasingly integrate healthcare services within broader consumer platforms, the complexity of HIPAA and the risks for noncompliant conduct will remain a significant concern and potential focus of regulatory attention.

Legal Background

The civil money penalty is due to violations of the HIPAA security rule. The OCR enforces the HIPAA privacy, security and breach notification rules. These rules delineate the requirements that covered entities — health plans, healthcare clearinghouses and most healthcare providers — and their business associates must follow to ensure the privacy and security of protected health information.

The HIPAA security rule created standards to protect individuals' electronic protected health information that is created, received, used, disclosed, maintained or transmitted by a covered entity, including administrative, physical and technical safeguards to ensure the confidentiality, integrity, availability and security of electronic protected health information.

The Warby Parker civil money penalty resolves the OCR's investigation following a breach investigation.

In an HHS press release from Feb. 20, OCR Acting Director Anthony Archeval stated that:

> identifying and addressing potential risks and vulnerabilities to electronic protected health information is necessary for effective cybersecurity and compliance with the HIPAA Security Rule. Protecting individuals' electronic health information means regulated entities need to be vigilant in implementing and complying with the Security Rule requirements before they experience a breach.[1]

Archeval's statement is a clear message that the OCR will evaluate security practices based on an entity's level of preparedness before a breach occurs, and reactive remediation may not be adequate.

The HHS secretary has the authority to impose civil money penalties, and the secretary has delegated the enforcement of these rules to the OCR director.

Pursuant to the Health Information Technology for Economic and Clinical Health Act, the OCR is authorized to impose civil money penalties, which will vary depending on the facts. According to HHS, civil money penalties will vary based on the type of violation and level of neglect.[2]

Each of the HITECH Act penalty thresholds are adjusted for inflation.

Warby Parker's Background

Warby Parker is a public benefit corporation based in Delaware and headquartered in New York. It has over 3,000 employees across approximately 200 stores. As a healthcare provider that transmits health information electronically, Warby Parker is a HIPAA covered entity.

On Nov. 26, 2018, Warby Parker became aware of unusual login attempts on its website. Warby Parker reported that between Sept. 25, 2018, and Nov. 30, 2018, unauthorized third parties gained access to their customer accounts by using usernames and passwords obtained from other, unrelated websites that were presumably breached. This type of cyberattack is often referred to as credential stuffing.

Warby Parker reported this breach to the OCR on Dec. 20, 2018, later amending the report on Sept. 18, 2020. The Warby Parker breach affected the electronic protected health information of 197,986 individuals, including customer names, email addresses, partial payment card information, and for most, eyewear prescription details.

Following Warby Parker's disclosure, the OCR initiated a breach investigation and Warby Parker's compliance with HIPAA in September 2019. Warby Parker experienced subsequent credential stuffing attacks in September 2019, January 2020, April 2020 and June 2022, breaching the information of 484 additional customers.

As noted in a HHS press release from Feb. 20, the OCR's investigation found evidence of three violations of the HIPAA security rule, including:

> a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to [electronic protected health information] in Warby Parker's systems; a failure to implement security measures sufficient to reduce the risks and vulnerabilities to [electronic protected health information] to a reasonable and appropriate level; and a failure to implement procedures to regularly review records of information system activity.[3]

According to the OCR, Warby Parker did not implement sufficient security measures to mitigate these risks until July 29, 2022. Furthermore, according to the OCR, Warby Parker failed to regularly review audit logs and security incident reports until May 12, 2020. These failures underscore common pitfalls in HIPAA compliance. Risk analysis and audit reviews should be continuous and active, not merely procedural exercises.

On March 14, 2024, the OCR informed Warby Parker of the investigation results and offered an opportunity to resolve the issue informally. A day later, the OCR issued a letter of opportunity to Warby Parker, outlining potential noncompliance with the security rule and requesting evidence for mitigating factors or affirmative defenses in determining potential civil money penalties.

Although Warby Parker responded to the letter of opportunity on June 14, 2024, the OCR found that their arguments did not support an affirmative defense and concluded that Warby Parker did not present sufficient evidence to waive the civil money penalty. On Aug. 13, 2024, the office issued Warby Parker a notice of proposed determination to impose a civil money penalty.

Determining the Amount of the Civil Money Penalty

In determining the civil money penalty amount, the OCR is required to consider certain factors, which may be mitigating or aggravating, as appropriate. The office determined that none of the factors listed below were aggravating or mitigating.

- The nature and extent of the violation;
- The nature and extent of the harm resulting from the violation;
- Warby Parker's history of prior compliance;
- The financial condition of Warby Parker; and
- Any other matters.[4]

The OCR is required to consider recognized security practices that HIPAA-covered entities adequately demonstrate had been in place for a period of no less than the previous 12 months when determining a civil money penalty.[5]

On Jan. 12, 2024, the office provided an opportunity for Warby Parker to adequately demonstrate that it had recognized security practices in place. Warby Parker responded to the office's request on Feb. 5, 2024. The office determined that Warby Parker did not demonstrate adequate implementation of recognized security practices for the required 12-month period.

Consequently, no reduction in the civil money penalty was applied. The OCR's analysis suggests that well-documented, long-standing practices must be in place to be an effective recognized security practice. Covered entities should not treat recognized security practices as a conceptual safe harbor, but rather they should be used as a strategic compliance asset that they actively maintain.

The office imposed the following civil money penalties for each Warby Parker violation, each based on reasonable cause.

1. Risk analysis: $700,000, calculated based on a 6-year period prior to the Notice of Proposed Determination (NPD) date.[6]

2. Risk management: $500,000, also calculated for a 6-year period before the NPD date.[7]

3. Information system activity review: $300,000, also calculated over a 6-year period prior to the NPD date.[8]

Warby Parker waived its right to a hearing and did not contest the office's $1.5 million civil money penalty.

Suggestions for Covered Entities and Business Associates

In its April 25 press release announcing the Warby Parker civil money penalty, the office noted there are multiple steps that parties can take to mitigate or prevent cyberthreats, including the following:

- "Identify where [electronic protected health information] is located in the organization, including how [electronic protected health information] 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 [electronic protected health information]."
- "Encrypt [electronic protected health information] in transit and at rest to guard against unauthorized access to [electronic protected health information] 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."[9]

Trying to See the Future

HHS recently announced plans to dramatically reduce its workforce, which will presumably include a reduction in OCR staffing. It is not yet known whether the Trump administration and its HHS OCR leadership will continue to aggressively pursue alleged HIPAA security and privacy rule violations by covered entities and business associates.

Cybersecurity remains an important issue within the healthcare delivery system, and cybersecurity threats are not a political issue. Regular monitoring of electronic protected health information consistent with the HIPAA security rule requirements is imperative.

Performing routine and thorough risk analyses are critical. Timely replies to protected health information requests are not only good customer service, but delays may result in an OCR investigation. Additionally, ransomware and phishing issues are prevalent, and HIPAA

settlements and/or civil money penalties are very lengthy and expensive processes.

All covered entities and their business associates need to stay vigilant against emerging and ongoing cybersecurity activities by bad actors to protect their protected health information, whether electronic or not.

Bruce Armon is a partner and the chair of the healthcare practice at Saul Ewing LLP.

Bunyad Bhatti is an associate at the firm.

[1] https://www.hhs.gov/press-room/penalty-against-warby-parker.html.

[2] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/pmi-npd/index.html.

[3] https://www.hhs.gov/press-room/penalty-against-warby-parker.html#:~:text=OCR's%20investigation%20found%20evidence%20of,to%20reduce%20the%20risks%20and.

[4] https://www.hhs.gov/sites/default/files/ocr-warby-parker-npd.pdf.

[5] Public Law 116-321. https://www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.

[6] 45 C.F.R. § 164.308(a)(1)(ii)(A).

[7] 45 C.F.R. § 164.308(a)(1)(ii)(B).

[8] 45 C.F.R. § 164.308(a)(1)(ii)(D).

[9] https://www.hhs.gov/press-room/ocr-hipaa-racap-np.html.