STRATEGIC MANAGEMENT SERVICES

HIPAA Cybersecurity Compliance:

Lessons From OCR'S Latest $1.5M Penalty

Sally A. Enoh | **March 2025**

Key Points:

- **Cybersecurity Gaps Lead to Significant Penalties**
- **Tips to mitigate cybersecurity risks**

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently imposed a $1.5 million civil money penalty against Warby Parker, Inc., following an investigation into violations of the HIPAA Security Rule. The action stems from a credential-stuffing cyberattack that resulted in unauthorized access to the protected health information (PHI) of nearly 200,000 individuals. This enforcement action serves as a critical reminder for covered entities and business associates under HIPAA to maintain robust cybersecurity measures and ensure compliance with risk management and system monitoring requirements. OCR's investigation began after Warby Parker reported a data breach caused by credential stuffing, a cyberattack in which hackers use stolen username-password combinations from unrelated websites to gain access to user accounts. The breach exposed sensitive customer data, including names, mailing addresses, email addresses, payment card information, and eyewear prescriptions. OCR found three key violations of the HIPAA Security Rule: (1) failure to conduct a comprehensive risk analysis to assess vulnerabilities to electronic PHI (ePHI); (2) failure to implement sufficient security measures to mitigate known risks; and (3) failure to regularly review system activity to detect potential threats. This case highlights the regulatory expectations for HIPAA-covered entities and business associates. OCR has consistently emphasized that proactive risk management is essential for safeguarding ePHI, particularly in an era of increasingly sophisticated cyberattacks.

Tips to Mitigate Cybersecurity Risks

1. **Conduct Regular Risk Assessments**: Identify vulnerabilities in information systems, ensuring ePHI is adequately protected against cyber threats.

2. **Implement Strong Access Controls**: Use multi-factor authentication (MFA) and advanced authentication mechanisms to prevent unauthorized access.
3. **Monitor and Audit System Activity**: Establish logging mechanisms to track and review system activity, ensuring early detection of suspicious behavior.
4. **Encrypt ePHI in Transit and at Rest**: Protect sensitive data through encryption to minimize the risk of unauthorized access.
5. **Strengthen Workforce Training**: Provide ongoing cybersecurity training to employees, ensuring they recognize security threats and follow best practices.
6. **Develop an Incident Response Plan**: Establish clear protocols for responding to cybersecurity incidents to minimize damage and ensure compliance.

For more information on this subject, contact the author, Sally Enoh, JD, MCRM, CHC, CHPC, at senoh@strategicm.com.

About the Author

Sally Enoh, a law school graduate with a master's in Healthcare Regulatory Compliance and Risk Management, is skilled in regulatory research and analysis of federal health care regulations including the False Claims Act, Anti-kickback Statute, and HIPAA Privacy and Security Rules. Ms. Enoh assists senior consultants on engagements, such as program development, implementation, evaluation, and management. Additionally, Ms. Enoh performs reviews of compliance programs, evaluates clients' adherence to Corporate Integrity Agreement requirements, and provides compliance advisory services.