OneHealth Risk Assessment Report

Prepared by: Melven Saint-Paulin

Date: May 22, 2025

Frameworks: NIST SP 800-30 | HIPAA Security Rule

# 1. Executive Summary

\*Please note this was a mock assessment done on my current employer. Names and sensitive info were made generic to avoid conflicts. \*

This risk assessment, conducted for OneHealth, evaluates key threats and vulnerabilities impacting its electronic healthcare infrastructure and company. Utilizing NIST SP 800-30 and HIPAA Security Rule guidelines, the assessment identifies, analyzes, and prioritizes risks across systems including EHR platforms, cloud infrastructure, mobile devices, and endpoint environments. Risk mitigation recommendations are provided to strengthen OneHealth’s information security posture.

# 2. Scope of Assessment

The scope of this assessment covers OneHealth’s critical technical and data assets, including the EHR web platform, backend application servers, cloud-hosted databases, access control mechanisms, and endpoints such as staff laptops and work phones. It also includes mobile access to protected health information (PHI), audit logs, and remote access mechanisms.

# 3. Frameworks Applied

This assessment adheres to the risk assessment methodology outlined in NIST SP 800-30 and aligns with safeguards required under the HIPAA Security Rule. The controls and recommendations are also mapped to common best practices derived from NIST SP 800-53 and security operations frameworks.

# 4. Methodology

Each asset was evaluated based on its associated threats and vulnerabilities. Risk scores were calculated using a standard Likelihood × Impact matrix (scale of 1–5), and risks were categorized as Low (≤9), Medium (10–15), or High (16–25). The most critical risks were prioritized for mitigation, and controls were assigned with responsible owners and deadlines.

# 5. Key Risk Findings

Highlighted risks include:  
- EHR systems susceptible to session hijacking due to weak session controls.  
- Sensitive PHI data lacking encryption at rest.  
- Mobile access to EHR without proper device compliance checks.  
- Privilege escalation risks within IAM roles and staff user profiles.  
- Exposure of cloud-hosted data due to misconfigured S3 bucket policies.  
A full risk register including 20 detailed entries is provided in the appendix.

# 6. Recommendations

It is recommended that OneHealth prioritize remediation of High risks within 30 days. This includes enforcing encryption for PHI data, applying MFA and session timeout configurations, deploying MDM on mobile devices, and implementing centralized logging and access controls. Medium and Low risks should be addressed based on resource availability and strategic priorities.

# 7. Conclusion

OneHealth has a modern and scalable technical environment, but improvements in endpoint security, cloud governance, and access control management are necessary to maintain HIPAA compliance and resilience against cybersecurity threats. This assessment provides a roadmap for strengthening security controls and reducing risk exposure.

# 8. Appendix

- Appendix A: Asset Inventory (Excel)  
- Appendix B: Threat & Vulnerability Matrix (Excel)  
- Appendix C: Risk Register (Excel)