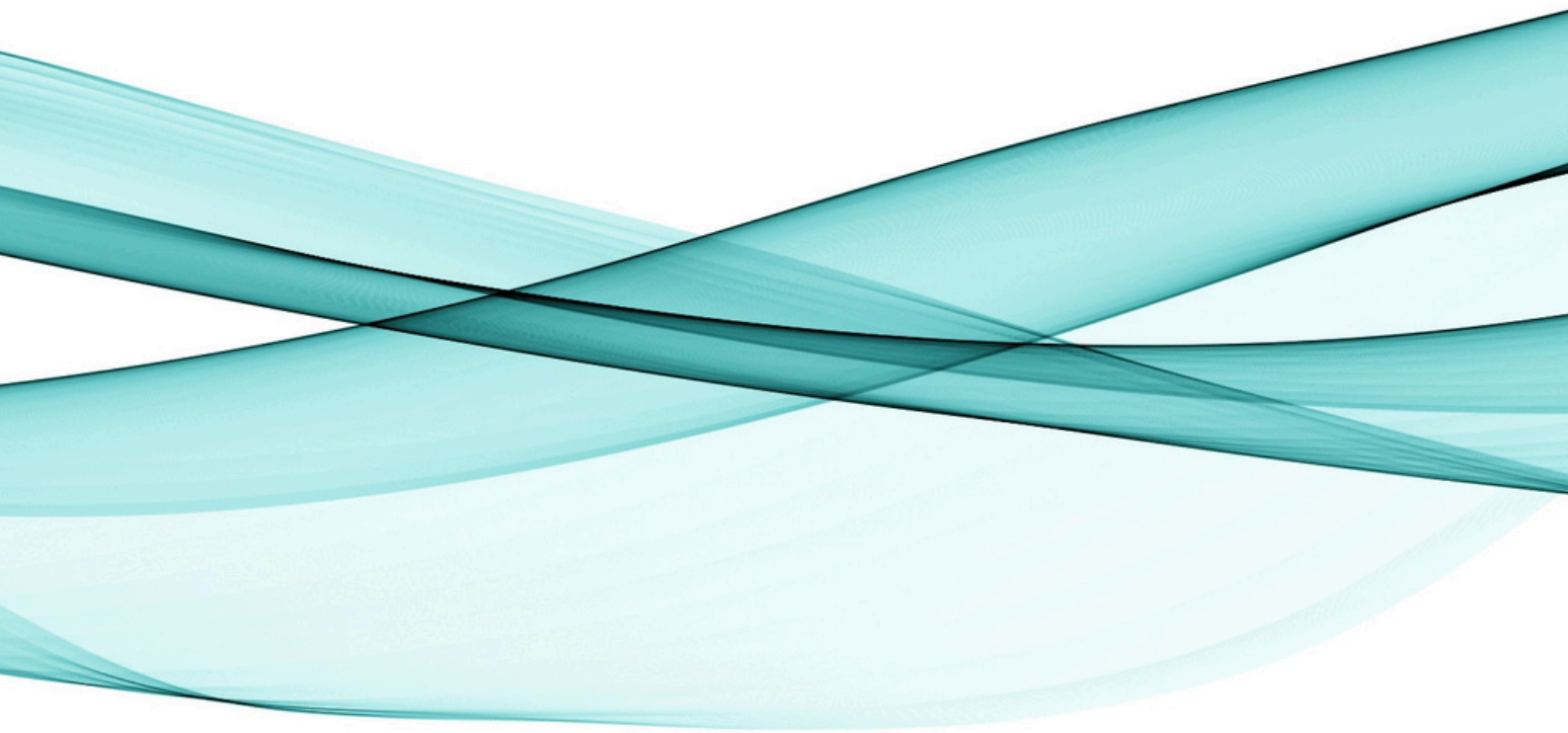


HIPAA Pentest Report



HIPAA Penetration Testing Assessment Report

1. Executive Summary

Securify performed a targeted HIPAA-focused penetration test for a U.S.-based digital health platform handling sensitive ePHI. The engagement focused on identifying exploitable weaknesses and validating the effectiveness of implemented safeguards.

The assessment revealed a mix of configuration issues, access control gaps, and minor application-layer weaknesses. All critical risks were addressed, resulting in a significantly improved security posture and compliance readiness.

2. Scope of Assessment

The testing scope included:

• Web application and APIs

• Cloud infrastructure and configurations

• Authentication and authorization controls

• Data transmission and encryption layers

3. Methodology

A black-box testing approach was used, simulating a real-world attacker with no prior access. The methodology followed OWASP testing standards and included reconnaissance, vulnerability identification, exploitation, and validation.

4. Risk Summary

Severity	Count	Description
Critical	1	High impact data exposure risk
High	2	Access control and injection risks
Medium	3	Configuration and validation gaps
Low	2	Security hardening issues

5. Key Findings Overview

The testing identified several vulnerabilities that could potentially impact data confidentiality and system integrity if exploited.

Examples include exposed endpoints, weak validation controls, and incomplete encryption enforcement.

6. Evidence Snapshot

During testing, multiple endpoints were analyzed and responses validated to confirm exploitability.

Example: API endpoint manipulation allowed retrieval of structured data responses, confirming improper access control enforcement.

Example: HTTP responses revealed missing security headers, increasing exposure to client-side attacks.

7. Remediation Actions

Securify collaborated with the internal team to resolve all identified issues. Key improvements included:

• Implementation of strict authentication and authorization

• Enforcement of HTTPS across all endpoints

• Input validation and secure coding enhancements

• Security headers and infrastructure hardening

8. Validation & Retesting

All critical and high vulnerabilities were retested post-remediation. The results confirmed that the issues were successfully mitigated and no longer exploitable.

9. Final Outcome

The organization achieved a strong security posture aligned with HIPAA expectations. The environment is now significantly more resilient against real-world attack scenarios.

10. Conclusion

Securify successfully delivered a structured and professional penetration testing engagement, ensuring both security assurance and compliance confidence for the client.