Borderless CS
CYBER SAFE TOGETHER

Circumcision Vasectomy Australia

Penetration Testing (Web & Mobile) and Source Code Review Customer success story

CLIENT: CIRCUMCISION VASECTOMY AUSTRALIA (CVA)

INDUSTRY: HEALTHCARE (PHI & PII)

CLIENT WEBSITE: https://circumcisionvasectomyaus.com.au/

SERVICE: Penetration Testing and Source Code Review

Customer Success Story

Circumcision Vasectomy Australia (CVA) Strengthens PHI & PII data Security with Borderless CS Through Comprehensive CREST Aligned Penetration Testing & Source Code Review

Overview

Circumcision Vasectomy Australia (CVA) is a specialised Australian healthcare provider offering circumcision, vasectomy, and men's reproductive health services. With a modern digital ecosystem comprising **mobile applications**, **a consolidated multi-role web platform**, and **backend API services**, CVA manages highly sensitive patient information — including PHI and PII.

As part of its commitment to clinical excellence and data protection, CVA engaged **Borderless CS** to conduct a **comprehensive CREST Aligned Penetration Testing and Source code review:**

Data Handled: PHI (Protected Health Information), PII (Personally Identifiable Information)

- **Mobile Application Penetration Testing (iOS & Android)**
- **Web Application Penetration Testing**
- **End-to-end Secure Source Code Review**

The goal was to identify security gaps, validate secure engineering practices, and ensure robust protection of patient data across all digital touchpoints.

Engagement Objectives

Borderless CS was commissioned with these core objectives:

1. **Identify vulnerabilities** across mobile apps, the web platform, and backend APIs.
2. **Ensure the security of PHI and PII** across all authentications, data storage, and transmission flows.
3. **Evaluate secure coding practices** through a deep-dive source code review.

4. **Assess role-based access controls**, business logic, and security boundaries within CVA's digital ecosystem.
5. **Provide a clear remediation roadmap** aligned with industry best practices and healthcare security standards.

Scope of Work

1. Mobile Application Penetration Testing (iOS & Android)

CVA's mobile applications required a full security evaluation across both platforms.

Testing covered:

Mobile Testing Components:

- Application binary analysis
- API communication security
- Authentication & session flows
- Encryption & secure local storage
- Business logic & RBAC validation
- Secure integration with backend systems

Testing followed **the OWASP Mobile Security Testing Guide (MSTG) and the OWASP Top 10 Mobile** frameworks.

2. Web Application Penetration Testing

CVA operates a unified web application supporting multiple roles and functions, including:

- Staff portal
- Admin portal
- Scheduling
- Patient management
- Backend management workflows

Testing covered:

Web Application Security Components

- Authentication & authorisation flows
- RBAC privilege escalation checks
- Session management
- Input validation & injection testing
- Encryption and data transmission security
- Backend APIs and endpoints
- Business logic abuse scenarios
- Data segregation & tenant isolation

Testing was conducted in accordance with OWASP ASVS, OWASP Top 10, and healthcare data security standards.

3. End-to-End Secure Source Code Review

Borderless CS performed a **deep-dive code review** across:

- Full backend codebase
- Frontend (web & mobile)
- API communication handlers

Source Code Review Components

- Manual secure code review of critical modules
- Static code analysis using industry tools
- Authentication & authorisation logic review
- API request/response validation
- Input sanitisation & output encoding
- Error handling & exception management
- Secrets & sensitive data exposure checks
- Hardcoded credentials, tokens, and API key analysis
- Third-party dependency & library risk assessment

The review followed **secure coding standards,** including OWASP, SEI CERT, and NIST secure software development guidelines.

Key Outcomes

1. Major Security Vulnerabilities Identified & Remediated

High-impact findings across authentication, API flows, and business logic were rapidly resolved.

2. Significantly Enhanced Protection of PHI & PII

Security controls were strengthened across all digital platforms handling sensitive patient data.

3. Hardened Mobile Apps (iOS & Android)

Vulnerabilities related to secure storage, transport encryption, and session handling were fully addressed.

4. A More Secure & Compliant Web Ecosystem

RBAC, session management, encryption, and backend API security were uplifted.

5. Improved Software Development Lifecycle (SDLC)

The source code review introduced secure coding patterns now embedded into development processes.

6. Executive-Level Security Roadmap Delivered

Borderless CS provided a clear, prioritised remediation roadmap aligned with healthcare cybersecurity standards.

Conclusion

By partnering with Borderless CS, **Circumcision Vasectomy Australia** (CVA) has significantly strengthened the security of its mobile apps, web platform, backend APIs, and overall software development practices.

This engagement ensures the organisation continues to protect patient PHI and PII with industry-leading security controls — reinforcing trust, compliance, and resilience as CVA expands its digital healthcare services across Australia.