
We follow a comprehensive **Secure Software Development Life Cycle (SSDLC)** aligned with **WordPress Coding Standards (WPCS)** and **OWASP best practices** to ensure the security, integrity, and confidentiality of patient data.

1. Requirements & Design
Security requirements are defined during the planning phase, including **HIPAA compliance** and **Role-Based Access Control (RBAC)**. The system is explicitly designed following the **Principle of Least Privilege**, ensuring users have only the minimum access required to perform their roles.

2. Development

- **Input Validation:** All API inputs are validated and sanitized using WordPress core functions such as `sanitize_text_field()` and `absint()`.
- **Authorization:** All REST API endpoints implement strict `permission_callback` checks to ensure that only authorized **Doctors** or **Administrators** can access sensitive features such as Zoom settings.
- **CSRF Protection:** WordPress nonces are verified for all state-changing requests to prevent Cross-Site Request Forgery (CSRF) attacks.

3. Testing
We perform **Static Application Security Testing (SAST)** using **PHP_CodeSniffer** with the **WordPress-Extra ruleset** to detect and prevent common vulnerabilities, including **Cross-Site Scripting (XSS)** and **SQL Injection (SQLi)**, during development.

4. Dependency Management
Third-party libraries are managed using **Composer**. All dependencies are regularly reviewed and kept up-to-date to ensure they are free from known security vulnerabilities (CVEs).
