

RxPx Security & Compliance Overview

Last updated: December 2025

1. Introduction

RxPx maintains and follows an Information Security Management System (ISMS) that is:

REGULATION-ALIGNED

Based on regional regulations including HIPAA, GDPR, APEC CBPR, and the Australian Privacy Act.

STANDARDS-INFORMED

Aligned with ISO 27001, ISO 9001, and ISO 13485, as well as frameworks like ITIL, OWASP, and COBIT.

OPERATIONAL

Guided by documented standard operating procedures for risk and compliance.

Security is integrated into the software development process via a documented **Secure Development Lifecycle (SDL)**, covering training, requirements, testing, and incident response.

2. Certifications

RxPx maintains the following active certifications:

CERTIFICATION	SCOPE
ISO 27001:2013	Information security management
ISO 9001:2015	Quality management systems
ISO 13485:2016	Quality management for medical devices

Note: A separate GDPR Compliance Statement is available for European data protection requirements.

3. Information Security Management System (ISMS)

The ISMS covers the following administrative, physical, and technical controls:

Security Management

Procedures for infrastructure changes, logging, and monitoring.

Risk Management

Defined processes for assessment and treatment of risks to confidentiality, integrity, and availability.

Access Control

Granular, per-resource authorization based on business need and security policy.

Security Awareness

Ongoing training for all employees and contractors relevant to their job functions.

Document Management

Governance over the storage and destruction of electronic and printed records.

Privacy Management

A dedicated plan for managing personal and health information (PII/PHI).

Physical Security

Protection of personnel and facilities from theft, damage, or unauthorized access.

Incident Response

A dedicated Incident Response Team to manage and communicate breaches with high priority.

Corrective Action

Procedures to ensure non-conformities are closed accurately and timely.

4. System and Software Security

4.1 Data Encryption

AT REST

Encrypted at two managed-key levels (AES-256) for block-level databases and server-side volumes/object storage.

IN TRANSIT

Encrypted using current TLS standards (TLS 1.2 in use; TLS 1.3 enabled) for both external and internal links.

4.2 Data Integrity & Privacy

PSEUDONYMIZATION

Used when processing data for purposes other than primary healthcare delivery or where explicit consent is absent.

ANALYTICS

Customer interfaces for reporting do not contain or display PII or PHI.

PASSWORD SECURITY

Stored as hashed values with unique salt using **PBKDF2 with HMAC-SHA**.

4.3 Resilience & Testing

SYSTEM INTEGRITY

Includes automated redundancy for High Availability (HA) and Disaster Recovery (DR) protocols.

INTERNAL TESTING

Regular automated and manual QA testing.

EXTERNAL PENETRATION

Annual third-party testing of front-end and back-end systems.

5. Recent Third-Party Attestations

RxPx has received Letters of Attestation from **Qualysec Technologies Pvt. Ltd.** for the following:

Chameleon Web Application

Assessment of patient and HCP-facing platforms

Dated: 27 Jan 2026

AWS Cloud Environment

Assessment of cloud infrastructure and environment

Dated: 22 Jan 2026

Legal & Contact Information

This document is for information purposes only. Responsibilities and liabilities are governed by separate customer agreements.

CONTACT
contact@rxpx.health
https://rxpx.health