Information Security Management System

Compliance Statement

Outcome Health is an ISO 27001 certified organisation. The ISO 27001 framework is internationally recognized as the cornerstone of an organisation's mature security posture. This document explains how Outcome Health's adherence to the ISO 27001 standard addresses primary security considerations.

Understanding our ISO 27001 certification

Our Commitment to Information Security
As a health data analytics company, Outcome Health recognises the critical importance of information security. Our ISO 27001 certification is tangible evidence of our commitment to managing and protecting data through a comprehensive **Information Security Management System (ISMS)**.

In practical terms, ISO 27001 is not just about implementing **individual controls**; rather it is about adopting a comprehensive **systems approach** which requires us to:
Identify Risks: involves regular assessment of potential threats and vulnerabilities to the data collected and processed across the POLAR platform.

Implement Controls: appropriate measures are in place to address identified risks. This covers technical controls (related to authentication, encryption, network security), physical security, and procedural controls (such as access management and incident response).

Monitor & Review: Continuous checks to ensure implemented controls are working effectively and update them as threats change or systems evolve.

Improve: **security isn't static**; it's an ongoing process of review and enhancement.

Our adherence to ISO 27001 is confirmation that key areas of technical and procedural security are systematically managed, including:
Infrastructure & Hosting: Our services are hosted on secure infrastructure within a certified data centre. ISO 27001 requires us to rigorously manage the security of this environment, including physical security, network controls, and resilience.

Authentication & Access Control: The standard mandates strong access control policies and mechanisms, covering aspects like secure authentication, management of user privileges, password policies, and account protection.

Data Protection: Fundamental to information security, ISO 27001 ensures we have defined processes and controls for data storage, encryption (at rest, in transit, backups), data backup regularity, testing, retention, and disaster recovery.

System Security & Maintenance: Operational security, including practices like security patching, system monitoring, and managing cybersecurity measures, falls under the scope of our ISMS.

Environments & APIs: Any distinct environments (e.g., production, non-production) or APIs for integration are managed securely as part of our overall ISMS.

Why This Matters:

Independent Verification: An accredited, independent auditor has confirmed that our security management system meets this comprehensive international standard.

Robust Security Baseline: Our certification provides a strong, validated baseline, demonstrating systematic attention to a wide array of security best practices.

Commitment to Security: It details our serious, ongoing commitment to protecting the de-identified health data we analyse.

In summary, the Outcome Health ISO 27001 certification confirms the organisation has adopted a robust, audited framework for managing information security. This framework mandates a systematic approach to addressing technical and procedural security controls, providing a strong baseline for security assurance.

Engagements for in-depth reviews or specific consultations beyond this overview are subject to a separate scope of works agreement.

Ethics

POLAR has standing ethics approval for the collection, transfer, processing and storage of data on the POLAR platform (RACGP NREEC Protocol Id: 17-008).