**Southern Motion Physiotherapy**  
**Compliance Gap Analysis**

**1. Introduction**

**Purpose**

To assess Southern Motion Physiotherapy's current information security and data protection practices against applicable laws, regulations, and cybersecurity standards to identify areas of non-compliance or improvement.

**Scope**

This gap analysis focuses on compliance with the following:

* Australian Privacy Principles (APPs)
* ACSC Essential Eight Maturity Model
* ISO/IEC 27001:2022 Information Security Management Standard
* Best practices in health data protection for small clinics

**2. Compliance Gap Analysis Matrix**

| **Standard/Requirement** | **Compliance Area** | **Current Status** | **Gap Identified** | **Recommended Action** | **Priority** |
| --- | --- | --- | --- | --- | --- |
| **APP 1**: Open and transparent management of personal information | Privacy Policy & Documentation | Partially Compliant | No publicly available privacy policy for patients | Publish a privacy policy on the clinic website and in clinic | High |
| **APP 6**: Use or disclosure of personal info | Third-party data handling | Non-Compliant | No documented controls for third-party access to patient data | Draft and enforce vendor data handling agreements | High |
| **APP 11**: Security of personal information | Access control, encryption | Compliant | – | Maintain current measures | Medium |
| **Essential Eight**: Application control | Device & software management | Partially Compliant | No standardised process for restricting unauthorised applications | Implement application whitelisting policies | High |
| **Essential Eight**: Patch management | OS and software updates | Partially Compliant | Irregular software patching, no tracking | Implement a patch management schedule | Medium |
| **Essential Eight**: MFA | Authentication controls | Compliant | – | Continue enforcing MFA across all systems | Medium |
| **Health Data Protection**: Staff training | Security awareness | Partially Compliant | Training occurs but is not documented | Track and document all training completion | Medium |
| **Health Data Protection**: Data backups | Business continuity | Compliant | – | Conduct routine restore tests | Medium |
| **OAIC Notification**: Breach notification | Incident response | Compliant | – | Review response plan annually | Low |
| **ISO 27001**: A.5.1 Policies for information security | Governance | Partially Compliant | No overarching ISMS policy documented | Develop and approve an Information Security Policy | High |
| **ISO 27001**: A.6.1.1 Information security roles and responsibilities | Risk and roles | Partially Compliant | Roles and responsibilities not clearly documented | Define and communicate security roles/responsibilities | Medium |
| **ISO 27001**: A.9.2.1 User registration and de-registration | Access control | Compliant | – | Periodically review user access | Low |
| **ISO 27001**: A.12.6.1 Technical vulnerability management | Patch management | Partially Compliant | No documented vulnerability management process | Implement and document vulnerability management procedures | High |
| **ISO 27001**: A.16.1.1 Responsibilities and procedures | Incident response | Compliant | – | Continue annual testing and updates to IRP | Low |

**3. Summary**

Southern Motion Physiotherapy has made commendable progress toward complying with relevant Australian privacy and cybersecurity frameworks. The clinic already meets key requirements around encryption, multi-factor authentication, and data backup. However, the gap analysis has revealed several important areas for improvement:

* Absence of a publicly available privacy policy
* No formal agreements in place for third-party data access
* Inconsistent patch and application management
* Training is not consistently documented
* No overarching Information Security Management System (ISMS) policy
* Security roles and responsibilities are not clearly defined
* Vulnerability management practices are not formally implemented

By addressing these areas, the clinic will significantly enhance its regulatory compliance posture and align more closely with ISO/IEC 27001 best practices.

A follow-up review is recommended within 6 months to track progress on these actions.

**Prepared by:** Amon Saysana  
**Date:** 18/5/2025