**Southern Motion Physiotherapy**  
**Risk Assessment Report**

**1. Overview**

This Risk Assessment Report identifies potential threats to Southern Motion Physiotherapy’s operations, evaluates their likelihood and impact, and outlines mitigation strategies. The goal is to proactively manage risks to protect patient data, ensure continuity of care, and maintain compliance with regulatory requirements.

**2. Risk Assessment Methodology**

We use a qualitative risk assessment matrix that considers:

* **Likelihood**: How probable it is the risk will occur (Low, Medium, High).
* **Impact**: The severity of consequences if the risk occurs (Low, Medium, High).
* **Risk Level**: A combination of likelihood and impact (Low, Medium, High).
* **Mitigation**: Measures to reduce the likelihood or impact.

**3. Risk Register**

| **Risk ID** | **Risk Description** | **Likelihood** | **Impact** | **Risk Level** | **Mitigation Strategy** |
| --- | --- | --- | --- | --- | --- |
| R1 | Ransomware attack | Medium | High | High | Regular data backups; staff phishing training; endpoint protection |
| R2 | Loss of patient data due to system failure | Medium | High | High | Daily backups; backup testing; redundant systems |
| R3 | Power outage | High | Medium | Medium | Uninterruptible Power Supply (UPS); backup site readiness |
| R4 | Unauthorised access to patient records | Medium | High | High | MFA; access control policy; regular audits |
| R5 | Insider threat (malicious or accidental) | Low | High | Medium | Staff training; strict user permissions; activity logging |
| R6 | Fire or physical damage to clinic | Low | High | Medium | Insurance; offsite backups; alternate work location |
| R7 | Non-compliance with privacy regulations | Medium | High | High | Regular privacy training; compliance checks; privacy officer oversight |
| R8 | IT vendor failure | Medium | Medium | Medium | Service Level Agreements (SLAs); alternative vendor options; regular vendor reviews |

**5. Recommendations**

* Conduct monthly audits on access control logs.
* Review and test backup systems quarterly.
* Update the acceptable use policy to address emerging threats.
* Evaluate cyber insurance coverage annually.
* Introduce phishing simulation training quarterly.
* Review vendor contracts to ensure disaster recovery obligations are included.