SightWatcher: Data Backup Policy

Purpose
This policy ensures the secure and reliable backup of all critical data to protect against data loss, corruption, or system failure. It outlines the procedures for performing, storing, and restoring backups.

Scope
This policy applies to all practice data, including patient records, financial data, business documents, and software necessary for operations.

Backup Procedures
All data is stored and backed up using cloud-based infrastructure provided by trusted vendors, that offer redundancy and high availability, including:

- Microsoft 365 and Azure cloud backup solutions
- Encrypted online backup services compliant with UK GDPR and NHS Digital standards
- Automatic backup retention policies managed by cloud service providers

Backup Storage and Security
Data backups are managed by Microsoft and other cloud service providers, ensuring:

- End-to-end encryption during data storage and transmission.
- Automated replication across geographically distributed data centers.
- Access control policies to prevent unauthorized data retrieval.

Backup Frequency
- Backups are conducted automatically by Microsoft and other cloud providers as per their standard retention policies.
- Backup retention and restoration policies align with industry best practices and regulatory requirements.

Restoration and Testing
- Cloud service providers conduct automated integrity checks on backups.
- Periodic tests are performed by the IT team to ensure recovery capability.
- Any restoration failures are escalated to the respective cloud service provider for resolution.

Compliance and Review

- This policy is reviewed **annually** or after significant IT changes.
- Staff are trained on backup procedures to ensure continuity in case of IT personnel absence.
- Compliance with **data protection regulations** is maintained at all times.

Responsibility

- The designated Data Protection Officer (DPO) oversees data security and cloud compliance.
- Cloud service providers (e.g., Microsoft) handle backup execution and data protection.
- IT personnel monitor backup success logs and escalate any issues for resolution.

By implementing this policy, we ensure the security, integrity, and availability of critical data essential to our operations.

Created by: Umar Vania
Updated Date: 20/02/2025

Approved by: Umar Vania
Next Review Date: 19/02/2026