DATA SECURITY AND PROTECTION POLICY

Version	Date	Version Created By	Version Approved By	Comments
V1	Oct 2017	LC	TA	Initial Policy
V2	Mar 2019	LC	TA	Replaces IG Toolkit - Updated and amended to DSPT

Contents

Appendices

1. Policy Statement

Surrey Physio Group recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information governance plays a key part in supporting clinical governance, service planning and performance management.

It also gives assurance to Surrey Physio and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

Surrey Physio will establish and maintain policies and procedures to ensure compliance with requirements contained within the Data Security and Protection Toolkit (DSPT)

2. Scope

This policy covers all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel information
- Organisational information

This policy covers all aspects of handling information, including (but not limited to):

- Structured record systems - paper and electronic
- Transmission of information - fax, e-mail, post and telephone

This policy covers all information systems purchased, developed and managed by/or on behalf of, the organisation and any individual directly employed or otherwise by the organisation.

3. Principles

Surrey Physio recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the Data Protection Act. Non-confidential information on Surrey Physio and its services will be available to the public through a variety of means, in line with Surrey Physio's code of openness. Work will be undertaken to ensure compliance with the Freedom of Information Act.

Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.

Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

Surrey Physio regards all identifiable personal information relating to patients as confidential, compliance with legal and regulatory framework will be achieved, monitored and maintained.

Surrey Physio regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

Surrey Physio will establish and maintain policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act.

Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.

Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable data security and protection controls are in place.

4. Information Security

Surrey Physio will establish and maintain policies for the effective and secure management of its information assets and resources.

Audits will be undertaken or commissioned to assess information and IT security arrangements.

Surrey Physio's Incident Reporting system will be used to report, monitor and investigate all breaches of confidentiality and security.

5. Information Quality Assurance

Surrey Physio will establish and maintain policies for information quality assurance and the effective management of records.

Audits will be undertaken or commissioned of Surrey Physio's quality of data and records management arrangements.

Practice Managers will be expected to take ownership of, and seek to improve, the quality of data within their services.

Wherever possible, information quality will be assured at the point of collection.

Surrey Physio will promote data quality through policies, procedures/user manual and training.

6. Legal and Trusted Related Policies

Surrey Physio has a comprehensive range of policies supporting the Data Security and Protection agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate. (Ref. Appendix 1)

7. Improvement Plan and Assessment

An assessment of compliance with requirements, within the Data Security and Protection (DSPT) will be undertaken each year. Annual reports and proposed action/development plans will be

presented to the Director of Surrey Physio for approval prior to submission to the DSPT. The requirements are grouped into the following initiatives:

- Code of Confidentiality
- Data Protection
- Freedom of Information
- Health Records
- Information Governance Management
- Information Quality Assurance
- Information Security

8. DSPT Management

Data Security and Protection management across the organisation will be co-ordinated by the Data Security and Management. The membership of this group will comprise:

- The Caldicott Guardian
- A Clinician - consultant grade
- The Data Protection Officer
- The Senior Information Risk Owner
- The Director of Surrey Physio

The responsibilities of the Data Security and Management will include (but not be limited to):

- Recommending for approval, by the appropriate Surrey Physio management, related policies and procedures.
- Recommending for approval to Surrey Physio Group Management the annual submission of compliance with requirements in the Data Security and Protection Toolkit and related action plan.
- To co-ordinate and monitor the Data Security and Protection Strategy across the organisation.

Data Security and Protection leads throughout the organisation will be central to the delivery of the data security and protection strategy.

9. Training

All staff should attend, as part of their induction, a training session on Data Security and Protection. Top–up training will be provided; this can be requested by an individual wanting personal development or arranged at the discretion of a manager.

Appendix 1

Surrey Physio Related Policies

- Data Protection Policy
- Access to Personal Health Records Policy
- Information Security Policy
- Data Sharing and Guidance Policy
- Lifecycle Policy
- Professional codes of conduct from the HSPC, CSP and GOC
- Quality Policy
- Training Policy
- GDPR Privacy Notice Policy

Legal Acts

- Data Protection Act 2018
- Human Rights Act 2000
- Freedom of Information 2000
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act)
- Computer Misuse Act 1990
- Copyright, designs and patents Act 1988 (as amended by the Copyright Computer programs regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000