PROCEDURE NAME	Data Protection Policy	**PROCEDURE NO.**	GDPR, 001
MANAGER RESPONSIBLE	Joanna Pollock	**VERSION NO.**	3.0
SIGNATURE		**APPROVALS DOCUMENT OWNER**	JP

VERSION HISTORY				
VERSION	**REVIEWED BY**	**ISSUE DATE**	**DESCRIPTION OF CHANGE**	**APPROVED BY**
2.0	Michéal O'Neill	19.05.2022	Updated and amended as per report of Arthur Cush.	MON
1.0	Máire Hussey, Úna Houlihan, Mandy McKenzie Vass, Ronan Enright	01.11.2018	All amendments completed and updated.	MH, UH, MMV, RE

1. INTRODUCTION

Data Protection is how the privacy rights of individuals are safeguarded in relation to the processing of their personal data. SouthDoc needs to collect and use personal data about its patients, members, staff, and other individuals who come into contact with the organisation. Those individuals, 'data subjects', have privacy rights in relation to the processing of their personal data. SouthDoc must therefore comply with the European General Data Protection Regulation (GDPR) and the Irish Data Protection Act (DPA).

2. PURPOSE

The objective of this Data Protection Policy is to set out the requirements of SouthDoc, and the measures we take to protect the rights of data subjects.

3. SCOPE

This policy applies to all SouthDoc staff, students, contractors, sub-contractors, agency staff and authorised third party commercial service providers when receiving, handling, or processing personal data as defined by the GDPR.

4. DEFINITIONS

A list of terms used throughout this policy are defined in Appendix 1.

5. PRINCIPLES OF DATA PROTECTION

All personal data shall be processed in accordance with the following principles according to Article 5 of the GDPR:

- Personal data shall only be processed lawfully, fairly, and in a transparent manner.
- Personal data shall only be collected for specified, explicit, and legitimate purposes and shall not be processed in any manner incompatible with those purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Personal data shall be accurate and up to date.
- Personal data shall not be kept for longer than is necessary for the purposes for which it is processed – and will be retained in line with the data retention policies.
- Personal data shall be processed in a secure manner and kept secure – which includes having appropriate protection against unlawful or unauthorised processing and against accidental loss, destruction, or damage.

SouthDoc shall be responsible for and must be able to demonstrate compliance with these key principles.

In addition, SouthDoc will ensure that data subject's rights are protected as set out in the GDPR.

- Data subjects will be able to request access to data we hold on them through a Subject Access Request (SAR).
- Data subjects can request to change or correct any inaccurate data.
- Data subjects have the right to object to having their personal data processed.
- Data subjects can request to delete data that we hold excluding medical records.
- Data subjects can request to have their data moved outside of SouthDoc if it is in an electronic format.
- Data subjects can object to a decision made by automated processing, with certain limited exceptions and request that any decision made by automated processes have some human element.

6. LAWFULLNESS OF PROCESSING DATA

Processing shall be lawful only if and to the extent that at least one of the following applies:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7. DATA STORAGE LIMITATION POLICY

SouthDoc shall erase any personal data that violates:

- Data Protection Law
- Data Protection Regulations
- Contractual Obligations
- Requirements of this Policy
- If SouthDoc no longer requires the Data

8. UNAUTHORISED DISCLOSURE

All persons covered under this policy are prohibited from disclosing a data subject's confidential information (including personal data or special categories of personal data) unless this policy or a legal basis allows for such disclosures.

All persons covered under this policy must report all suspected incidents of unauthorised access to the DPO in line with the Data Breach Policy. Incidents include disclosure, loss, destruction or alteration of patient and service user's personal information, regardless of whether it is in paper or electronic form.

9. PRIVACY BY DESIGN OR DEFAULT AND DATA PROTECTION IMPACT ASSESSMENTS

If SouthDoc engages in a new data processing activity or if the processing activity is likely to increase the risk of a data breach, then they should:

- Engage the DPO for guidance
- Conduct a mandatory Data Protection Impact Assessment (DPIA)

A DPIA is a process which systematically considers the potential impact of a project and helps you to identify and minimise the data protection risks of a project.

SouthDoc adopts privacy by design as a default approach.

10. INFORMING PATIENTS OF THEIR PRIVACY RIGHTS

The organisation has put together an advisory note guiding patients of their privacy rights when providing personal data. This notice is available on the SouthDoc website and within Treatment Centres.

11. THIRD PARTY PROCESSORS AND DATA PROCESSING AGREEMENTS

A data processor is a third-party person or organisation that holds or processes personal data on the behalf of SouthDoc.

Prior to engaging with data processors, SouthDoc must ensure the following:

- Ensure it is appropriate to engage the Data Processor
- Ensure the data processor puts in place an agreement in writing (Data Processing Agreement) that complies with the requirements under data protection law.

If there are any changes to the way data is being processed or held, the data controller must be advised immediately by the data processor.

If the data processor must secure prior approval if they wish to engage further data processors.

At the expiry of a data processor contract the data processor is contractually obliged to return the full data set and provide unequivocal evidence that their copy of the dataset is erased.

12. TRANSFER OF PERSONAL DATA OUTSIDE EEA

SouthDoc must not transfer personal data to a third party outside of the EEA unless:

- The EU recognises the transfer country/ territory ass having an adequate level of data subject legal protection relating to personal data processing.
- The data subject has explicitly consented to the transfer of data or transfer is authorised by law.

13. EDUCATION

SouthDoc ensures that data protection training and guidelines are provided to all personnel.

As new articles, advice and points of interest are identified these are uploaded to the Intranet for all staff to access.

14. ROLES AND RESPONSIBILITIES

Data Protection Officer
Under the GDPR, certain organisations are required to appointment a designated Data Protection Officer (DPO). The duties of DPO are as follows:

- Support programmes of work from inception to ensure that data protection is addressed by default and in the design of new systems and information processes.
- Liaise with the supervisory authority.
- To ensure that the organisation can demonstrate compliance with all aspects of GDPR.
- To be available to be contacted directly by data subjects.

Employee Responsibilities
Compliance with data protection legislation is both a personal and an organisational responsibility. To ensure that personal and special categories data is secure, staff should:

- Follow the policies and procedures put in place to prevent unauthorised access, loss, theft, or alteration.
- Talk to their manager or DPO if they have any questions or concerns.
- Ensure any suspicious emails and / or breaches are reported immediately.

SouthDoc reserves the right to take such action as it deems appropriate against individuals who breach the conditions of this policy. If a breach occurs due to reckless behaviour and a breach occurs and is knowingly not reported, the person responsible may be held accountable.

15. ASSOCIATED DOCUMENTS

The following documents will provide additional information:

- Records Management Policy
- CCTV Policy
- Data Breach Policy
- Freedom of Information Policy
- Subject Access Request Procedure
- Data Security Policy

16. POINTS OF CONTACT

The first point of contact for any queries or requests should be directed to the DPO at SouthDoc Head Office.

Email: dpo@southdoc.ie

Phone: 064 6691974

Postal address: Data Protection Officer,
Floors 2&3 Hillard House,
High Street,
Killarney,
Co. Kerry
V93 K0DN

If one requires additional information on Data Protection, they should contact the Office of the Data Protection Commissioner (The supervisory authority).

Email: dpo@dataprotection.ie

Lo call number: 1800 437 737

Postal address: Data Protection Commission,
21 Fitzwilliam Square South,
Dublin 2,
D02 RD28

SOUTHDOC
out of hours family doctor service

APPENDIX 1: DEFINITIONS

Consent
A freely given, specific, informed and inambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

Data
In this policy 'data' shall mean information which either:

- is processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filling system or with the intention that it should form part of a relevant filling system;
- does not fall within any of the above, but forms part of a readily accessible record.

Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a relevant filling system.

Data Controller
A person or organisation who determines the purposes and methods of processing personal data.

Data Processing
The term 'processing' refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing, and destroying personal data – and can involve manual and electronic operations.

Data Processor
A person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data.

Data Protection
The protection of personal data.

Data Protection Commission (DPC)
The DPC is the Irish supervisory authority for the GDPR and also has functions and powers related to other regulatory frameworks including the Irish ePrivacy Regulations (2011) and the EU directive known as the Law Enforcement Directive.

Data Protection Officer (DPO)
The role within a company whose responsibility is to ensure that the company or organisation is correctly protecting individuals' personal data according to current legislation.

Data Subject
A living individual to whom personal data held relates, including: employees, patients, suppliers. It should be noted that GDPR do not apply to deceased persons and to their data.

Personal Data
Personal data is any information relating to an identified or identifiable living person (data subject) who could be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location, DOB, or to one or more factors specific to the physical, physiological, genetic, economic, cultural, or social identity of that individual.

Personal Data Breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Special Category Data
GDPR provides extra protection for certain categories of personal data, called 'special category data' – referring to data which reveals:
"Racial or ethic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

These categories of personal data shall not be processed unless a controller can avail of one of the exceptions under Article 9 (2) of the GDPR.

Subject Access Request (SAR)
A written request made to the data controller by any individual about whom a data controller keeps personal data on computer on in a relevant filling system. Response must be provided to the data subject under the terms outlined by GDPR and/ or local requirements.

Third Party
Under GDPR, 'third party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who under the direct authority of the data controller or processor are authorised to process personal data.