

Data Protection Policy and Procedure

Document Control Sheet Title:	Data Protection Policy and Procedure
Implementation Date:	July 2022
Review Date:	July 2023
Author(s)	Simon Sinclair, Angela James
Senior Information Risk Owner:	Simon Sinclair (Director)
Data Protection Officer:	Simon Sinclair (Director)
Caldicott Guardian:	Angela James
Version No.:	4

Document Amendment History Version No.	Date	Brief Description
Version 1	June 2020	New Policy
Version 2	February 2021	Revised Policy
Version 3	February 2022	Policy Reviewed
Version 4	June 2022	Revised Policy

Synergy Complex Care Limited is registered under the Data Protection Act 2018.

Data Protection Registration number: ZA763851

This policy is to be read in conjunction with the Synergy Complex Care:

Code of Conduct

Confidentiality Policy

Information Governance Policy

Information Technology & Communication Policy and Procedures

Document & Data Retention Policy

Data Protection Policy and Procedure

1. Policy Statement

Synergy Complex Care holds personal data about employees and clients. Employment contracts contain a consent clause that gives permission for the data to be used as set out in the contract. If this information changes, employees have a duty to advise Synergy Complex Care so that records can be updated. Clients give consent for data to be used in order to provide contracted services.

Synergy Complex Care will follow its statutory obligations with regard to Data Protection and will notify the Information Commissioner's Office (ICO) that it is doing so.

Synergy Complex Care will comply with the eight principles of good practice:

1. To process data fairly and lawfully
2. To obtain personal data only for specified and lawful purposes and further process it only in a compatible manner
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and up to date
5. Personal data must be kept no longer than necessary
6. Personal data must be processed in accordance with the rights of the individual
7. Personal data must be kept secure
8. Personal data must only be transferred outside the EEA (European Economic Area) if there is adequate protection. (Ref: **Data Protection Act (DPA) 2018** Principle 8: Personal information is not transferred out of the EEA or to countries not authorised by the ICO)

Synergy Complex Care will ensure that the information it processes meets the relevant condition from the following:

1. The individual has consented to the processing
2. Processing is necessary for the performance of a contract with the individual
3. Processing is required under a legal obligation (other than one imposed by the contract)
4. Processing is necessary to protect the vital interests of the individual
5. Processing is necessary to carry out public functions e.g. administration of justice
6. Processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual)

At all times information is only to be provided on a strict 'need to know' basis.

Synergy Complex Care has reviewed the level of data that is held. As the company processes information about living people and processes data on behalf of clients such as CCG's.

The company has appointed the Director as the Data Protection Officer (encompassing the roles of the Data Controller and Data Processor) as required by the **General Data Protection Regulation (GDPR) 2018**. However, the company is not a Public Authority nor does it carry out large scale systematic monitoring of individuals, or large-scale processing of special categories of data.



The company has appointed the Registered Manager as the Caldicott Guardian (the senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly).

National Data Opt-Out

Synergy Complex Care reviews all of our data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies.

If any data processing falls within scope of the National Data Opt-Out we will use MESH to check if any of our service users have opted out of their data being used for this purpose.

2. Scope

This policy covers records held and processed by the Synergy Complex Care and is responsible for its own records under the terms of the DPA.

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

- Commissioners, Staff and Client information
- Personal information
- Organisational information

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

- Structured and unstructured record systems, paper and electronic
- Transmission of information by email, post, text and telephone
- Information systems managed by or used by Synergy Complex Care

3. Responsibility

While you are at work you may have access to information about clients/colleagues and/or Synergy Complex Care. You may come in to contact with this type of information during the course of your work or simply see, hear or read something while you are working. In these circumstances where duty of care, either to the client or the staff member overrides the duty of confidentiality, you must discuss the matter immediately with Registered Manager or the Director (Senior Information Risk Owner). Otherwise, you must keep this information confidential.

As an employee of the Synergy Complex Care Group you are subject to an obligation of confidentiality and must adhere to the Data Protection Act and Synergy Complex Care Data Protection and Confidentiality Procedures which form part of all employees Terms and Conditions of Employment.

Any changes or omissions to information must be reported to the Registered Manager or the Director (Senior Information Risk Owner).



All employees will receive training and familiarisation on Data Protection and Confidentiality and must sign a copy of Synergy Complex Care's Information Security Declaration (Appendix 1) without exception. Where appropriate this stipulation will apply to contractors and other third parties.

All employees will undertake mandatory refresher training at regular intervals or in line with changes to legislation and best practice. The company will monitor all staff's training records and ensure that update training where necessary will be carried out.

Any unauthorised disclosure of information by a member of staff will be considered as a disciplinary offence and will be subject to Synergy Complex Care's Disciplinary Policy.

4. Procedure for ensuring safe transfer of information

Principle 7 of the DPA legislates that all personal data must be kept secure. Therefore, every member of staff has an obligation to request proof of identity before confidential personal information is passed on. Every member of staff is personally responsible to take precautions to ensure the security of confidential personal information both whilst it is in their possession and when it is being transferred from one person or organisation to another.

Wherever possible all confidential information should be recorded using the company Care Management Software which is cloud-based, two-factor authenticated, encrypted and password protected.

The following is a list of recommended procedures to ensure the safe transfer of information should this not be possible:

1. Envelopes must be securely sealed, clearly addressed to a known contact and marked "confidential" and "addressee only". A return post code should also be marked on the envelope.
2. Telephone validation or "call back" procedures must be followed before disclosing information to someone you do not know to confirm their identity and authorisation.
3. Fax transfer is not safe and should be avoided.
4. Data (including confidential client information) must not be transferred/downloaded to portable electronic media.
5. E-mailing client confidential information is only permitted if it is encrypted or sent via NHS.net accounts.
6. Confidential client information must not be transmitted via the internet without it being encrypted or password protected, or where system-to-system networks are known to be secure (e.g. NHS.net to NHS.net)
7. When anonymised, redacted or pseudonymised information is shared, care should be taken to ensure that the method used is effective and individuals cannot be identified from the limited data set e.g. age and postcode together could be sufficient enough to reveal an individual's identity.
8. Printing of confidential client information must take place in a secure location and under the supervision of the permitted individual.
9. Confidential client information, portable computers, care case notes or files must not be left unattended in cars, other Client's houses or in easily accessible areas.



10. Client information must not be left on computer screens when the computer is unattended and all computers must have their screen saver facility applied and secured by password.

5. Sensitive data

Specific provision is made under the Data Protection Act 2018 for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

For personal information to be considered fairly processed, at least one of several extra conditions must be met.

These include:

- Having the explicit consent of the individual
- Being required by law to process the information for employment purposes
- Needing to process the information in order to protect the vital interests of the individual or another person
- Dealing with the administration of justice or legal proceedings

6. Review of data held, storage and disposal of data

Synergy Complex Care holds personal data about clients and staff in appropriate detail to ensure that they provide a safe and secure service to the clients who are being cared for. The data is used to ensure that the staff allocated to carry out the services that have been contracted by clients have the skills to deliver the services.

Synergy Complex Care will ensure that records, whether manual or computerised, are held securely and safely. Adequate, secure facilities will be made available for the storage of manual records. All files and portable equipment must be stored under lock and key when not actually being used.

Access to manual records will be the responsibility of the Registered Manager or the Director (Senior Information Risk Owner) or their designated deputies, and any request for access must be made to them. They have the right to refuse access to records and will give their reasons, verbally or in writing, for doing so.

Computerised records will be protected by the issuing of user numbers and passwords to individuals. These are for the sole use of the person to whom they apply and any misuse may lead to disciplinary action resulting in dismissal.

Computerised records will be protected through the use of automatically updated antivirus and malware software, firewalls and monitoring systems.



Encrypted, strong authenticated and password protected cloud-based storage will be used for all data access (e.g. Windows365, Care Management and Scheduling systems).

Any and all information relating to employees remains the property of Synergy Complex Care.

Information will not be kept for longer than is necessary for the purposes of providing the service or meeting regulatory requirements. It is worth noting that the services that the company delivers to clients requires data to be held for many years due to the nature of the services provided by the company. **Refer to the Synergy Complex Care Document and Data Retention Policy for full details.**

All paperwork containing client or employee information will be subject to shredding and secure disposal. Disposal Certificates for the shredding of confidential data are held at each office location.

All electronic records containing client or employee information will be subject to deletion and over-writing in a timely manner.

Synergy Complex Care are Data Security and Protection registered and update the toolkit annually.

7. Disclosure of confidential information

You must not give any other person confidential information to which you have had access to in the course of your employment within the office or client home.

All information relating to Synergy Complex Care, its Clients and employees, however stored, is classed as the property of Synergy Complex Care and you must not keep or discuss such information, nor use it for your own purposes.

Failure to adhere to the above statements may result in disciplinary action being taken and may lead to your dismissal.

8. Disclosure exemptions under the DPA

In certain circumstances personal information may be disclosed, however it is vital that staff make an assessment of the need to disclose the information and document that the information has been released to whom for what reason. Further guidance is available from Registered Manager or Director who will advise on appropriate disclosure and approve/block access as required. For example, where an individual leaves the company, changes role or if information needs to be updated.

It is important to note that personal identifiable information permitted to be released in the above circumstances must remain compliant with the remaining Data Protection Principles:



- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

9. Non-compliance of Data Protection Policy

A breach of this policy in your use of Synergy Complex Care's information will be considered a serious disciplinary matter and will be dealt with accordingly. Examples of offences which may be considered to be gross misconduct (the list is not exhaustive) which may result in immediate dismissal are:

1. Unlawful disclosure of Personal Data and Sensitive Personal Data
2. Inappropriate use of Personal Data and Sensitive Personal Data
3. Accessing patient or staff personal data including medical records in the absence of a legitimate professional relationship
4. Misuse of the Personal Data and Sensitive Personal Data which results in any claim being made against Synergy Complex Care

All employees (and contractors, third parties) are required to report potential breaches to the Senior Information Risk Owner.

10. Response to Data Security Incidents

In the event of a breach the Senior Information Risk Owner will implement a breach-management plan which will include:

1. Containment and recovery – creation of a recovery plan and, where necessary, procedures for damage limitation.
2. Risk Assessment – to include the potential adverse consequences for individuals; how serious or substantial these are; and how likely they are to happen.
3. Notification – clarification about who needs to be notified and why. This may include the individual(s) concerned; the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.



4. Evaluation and response – the causes of the breach will be investigated thoroughly, as will our response to it. Policies and procedures will be updated and audited as required.

11. Subject Access Requests (SAR)

The GDPR grants the right of access to personal data to enable a data subject to check what personal data is being held, and to ensure that it is being lawfully processed. Any SAR by data subjects to obtain information must be passed to the Director (Senior Information Risk Owner). There is no fee payable to the company for processing a SAR and the time limit to respond has been limited to within one month and without reasonable delay.

12. Training

All employees will complete 'Handling Information - GDPR & Data Protection' and undertake mandatory refresher training at regular intervals or in line with changes to legislation and best practice.

The company will monitor all staff's training records and ensure that update training where necessary will be carried out.



Appendix 1

Information Security Declaration Form

Please detach and return this signed form to the Registered Manager.

All employees granted Internet access with company facilities must be provided with a written copy of this policy.

All Internet users must sign the following statement:

"I have received a written copy of Synergy Complex Care's Data Protection Policy.

I fully understand the terms of this policy and agree to abide by them. I realize that the company's security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file.

I acknowledge that any messages I send or receive may be recorded and stored in an archive file for management use.

I know that any violation of this policy could lead to dismissal or even criminal prosecution."

Please Print Name:

Signed:

Dated:

