

Confidentiality Policy

Document Control Sheet Title:	Confidentiality Policy
Implementation Date:	June 2022
Review Date:	June 2023
Author(s)	Simon Sinclair, Angela James
Version No.:	3

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

This policy is to be read in conjunction with the Synergy Complex Care:
 Code of Conduct
 Data Protection Policy
 Information Governance Policy
 Information Technology & Communication Policy and Procedures
 Document & Data Retention Policy

Confidentiality Policy

Purpose

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within Synergy Complex Care and have access to person-identifiable information or confidential information.

All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in Synergy Complex Care are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the European General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

It is important that Synergy Complex Care protect and safeguard person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant mandatory requirements and to provide assurance to commissioners and clients.

This policy sets out the requirements placed on all staff when sharing information within the Synergy Complex Care and between Synergy Complex Care, the NHS and non-NHS organisations.

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

Definitions of confidential information can be found in Appendix C.

All breaches of this policy should be reported immediately to the Registered Manager or Director.



1. Scope

All staff, without exception, are within the scope of this policy

2. Roles and Responsibilities

1. The Director has overall responsibility for strategic and operational management, including ensuring that Synergy Complex Care policies comply with all legal, statutory and good practice guidance requirements.
2. The Director is the Senior Information Risk Owner and takes take accountability for risk-based decisions and reviews with regards to the use, disclosure or processing of confidential data
3. The Registered Manager is the Synergy Complex Care Caldicott Guardian and is responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing by providing advice to professionals and staff.
4. Synergy Complex Care 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; therefore have not appointed a Data Protection Officer (DPO).
5. Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure.
6. Staff: Confidentiality is an obligation for all staff. Staff should note that they are bound by the Confidentiality clause in their contract and it is mandatory to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues. Any breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported to the Registered Manager.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

- (a) to obtain or disclose personal data without the consent of the controller
- (b) to procure the disclosure of personal data to another person without the consent of the controller, or
- (c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained. Any breach of confidentiality, inappropriate use of health data, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract, and must be reported to the Registered Manager

3. Principles

All staff must ensure that the following principles are adhered to:

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.



- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with the Registered Manager.

Synergy Complex Care is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever appropriate, in line with the data protection principles stated in the Data Protection Policy, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the Information Commission Office's Anonymisation Code of Practice.

Access to rooms and offices where terminals are present, or person-identifiable or confidential information is stored is controlled. Doors are locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

Synergy Complex Care's Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

4. Disclosing Personal/Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice (<https://ico.org.uk/>).



- When the information is required by law or under a court order. In this situation staff must raise in the first place with the Director who will advise on the appropriate actions.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent.

Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must raise in the first place with the Director who will advise on the appropriate actions.

If staff have any concerns about disclosing information they must raise in the first place with the Registered Manager.

Care must be taken in transferring information to ensure that the method used is as secure as it can be.

When transferring patient information or other confidential information by email, services or methods that meet NHS Encryption standards must be used. Emails between NHS Mail accounts meet this requirement (nhs.net to nhs.net). Emails between NHS Mail and other secure government domains also meet this requirement (e.g. gov.uk). Staff should seek advice when intending to send confidential information by email to a non-nhs.net address.

It is not permitted to include confidential or sensitive information in the body of an email. When e-mailing to addresses other than the secure domains described above the information must be sent as an encrypted attachment with a strong password communicated through a different channel or agreed in advance.

When communicating via the secure domains, to protect against the risk of accidentally sending to an incorrect recipient, the data should be sent in a password protected attachment, again with the password communicated through a different channel or agreed in advance.

5. Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. The taking home or removing of paper documents that contain person-identifiable or confidential information needs to be approved by the Registered Manager or Director.

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations.

If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of buildings.
- Confidential information is kept out of sight whilst being transported.



If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account.

Staff must not use or store person-identifiable or confidential information on a privately-owned computer or device.

6. Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal. This could also constitute an offence under the Computer Misuse Act 1990.

7. Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about themselves without a legitimate purpose.

Under no circumstances should employees access records about their own family, friends or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures.

If staff have concerns about this issue they should discuss it with their Line Manager, Corporate Information Governance Team or DPO.

8. Confidentiality Audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their



systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Registered Manager through a programme of audits.

9. Distribution and Implementation

This document will be made available to all staff via the intranet site. A notice will be issued in the staff bulletin notifying of the release of this document.

10. Monitoring

Compliance with the policies and procedures laid down in this document will be monitored by the Senior Management Team and may be subject to internal and external audit.

11. Equality Impact Assessment

This document forms part of Synergy Complex Care's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

12. National Data Opt-Out

At this time, we do not share any data for planning or research purposes for which the national data opt-out would apply. We review all of the confidential patient information we process on an annual basis to see if this is used for research and planning purposes. If it is, then individuals can decide to stop their information being shared for this purpose. You can find out more information at <https://www.nhs.uk/your-nhs-data-matters/>.



Appendix A: Confidentiality Do's and Don'ts

Do's

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS England or NHS Improvement.
- Do clear your desk at the end of each day, keeping all non-digital records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gov.uk. For up to date information of secure domains please contact the Corporate IG Team.
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.



Appendix B: Summary of Legal and NHS Mandated Frameworks

Synergy Complex Care is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of Synergy Complex Care, who may be held personally accountable for any breaches of information security for which they may be held responsible. Synergy Complex Care shall comply with the following legislation and guidance as appropriate:

The **European Data Protection Regulation (GDPR) and Data Protection Act (2018)** regulate the use of “personal data” and sets out eight principles to ensure that personal data is:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and where necessary kept up to date.
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The **Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews** recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared:

- Justify the purpose for using patient-identifiable information.
- Don't use patient identifiable information unless it is absolutely necessary.
- Use the minimum necessary patient-identifiable information.
- Access to patient-identifiable information should be on a strict need to know basis.
- Everyone should be aware of their responsibilities.
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect patient confidentiality.

Article 8 of the Human Rights Act (1998) refers to an individual's “right to respect for their private and family life, for their home and for their correspondence”. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The **Computer Misuse Act (1990)** makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access to data or programs held on a computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
3. Unauthorised acts with intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.
 - a. Making, supplying or obtaining articles for use in offences 1-3



Appendix C: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Special categories of personal information (previously known as 'sensitive' personal data) as defined by the Data Protection Act 2018 refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

