South East Coast Ambulance Service NHS
NHS Foundation Trust

Transmission and Secure Storage of Confidential Information (SafeHaven) Policy

Contents

Introduction

1.1. Patients, their families and staff have a right to believe and expect that private and personal information given in confidence will be used for the purposes for which it was originally given, and not disclosed to others without their consent, unless other legal obligations override this right. These rights are enshrined in Article 8 of the Human Rights Act 1998, the Data Protection Act 2018 / UK General Data Protection Regulation and supported within the NHS by the Caldicott principles.

1.2. All staff in South East Coast Ambulance Service NHS Foundation Trust (the Trust) have contractual obligations to safeguard the confidentiality, integrity and availability of Person-Identifiable Data (PID). This includes patient and employee information.

1.3. No employee of the Trust, its commercial partners or volunteer groups may share patient identifiable information unless it can be justified, on a need to know basis to support patient care; or there is a legal requirement / legal basis to disclose the information.

2. Aims and Objectives.

2.1. The aim of the policy is to ensure that person-identifiable information is transferred in a confidential and secure manner and that information is disclosed only when necessary.

2.2. This includes having one designated contact point at each site where confidential information is either stored or received. This is known as a 'Safe Haven'. All person-identifiable data (PID) exchanged between NHS organisations must pass between Safe Haven contact points.

2.3. **Details of these are listed at:**

2.3.1. https://digital.nhs.uk/services/organisation-data-service/file-downloads/safe-haven-directory

2.3.2. All members of staff must be made aware of the policies and procedures surrounding Safe Haven access.

2.3.3. The objective is to raise awareness with all Trust staff for the need to adopt appropriate measures to safeguard confidential information in storage and in transit.

2.4. **Safe Haven principles cover data held and transmitted by:**

- Fax machines.
- Post / e-mail / MS Teams.
- Telephones/ Answer phones.

- Computer Systems/ Electronic media.
- Manual records and books.
- Electronic White boards/ Notice boards etc.

3. Definitions

3.1. **Safe Haven** - The term safe haven is a location (or piece of equipment) located on Trust premises where arrangements are in place to ensure that person identifiable information can be held, received and communicated securely.

3.2. **PID** - Person Identifiable Data. This means information that alone or together with other information can lead to the identity of an individual.

4. Policy Statement.

4.1. The Trust will operate Safe-Haven procedures for flows of patient identifiable information in line with the NHS Caldicott Principles:

- **Principle 1** - Justify the purpose for using confidential information
- **Principle 2** - Only use it when absolutely necessary.
- **Principle 3** - Use the minimum that is required.
- **Principle 4** - Access will be on a strict need to know basis.
- **Principle 5** - Everyone must understand their responsibilities.
- **Principle 6** - Understand and comply with the law.
- **Principle 7** - The duty to share information can be as important as the duty to protect patient confidentiality.
- **Principle 8** - Inform patients and service users about how their confidential information is used.

4.2. Role Based Access controls and registered access levels to these flows will be agreed by the Caldicott Guardian.

4.3. Guidance posters will be placed in appropriate locations throughout the Trust (see appendices 2 – 4).

4.4. Mandatory annual Data Protection and Cyber Security Awareness training for all staff will include awareness of patient confidentiality and Safe Haven procedures.

4.5. The Information Governance Working Group (IGWG) in collaboration with the Trusts IG department will review information flows on an annual basis or when new flows are identified.

5. Arrangements

5.1. Safe Haven Location and Security Arrangements.

5.2. A Safe Haven location must be a room that has appropriate physical access controls in place or;

5.3. If sited on the ground floor any windows must have locks on them.

5.4. The room must conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.

5.5. Manual paper records containing person-identifiable information must be stored securely.

5.6. Computers must be not left on view or accessible to unauthorised staff and must be locked, logged off or powered down when not in use.

5.7. **Fax Machines**

5.7.1. The Trust has one dedicated Fax Machine which is located within the 111 Service in Ashford.

5.7.2. Fax machines must only be used in exceptional circumstances to transfer personal information where no other secure option is available. The following rules must apply:

5.7.3. A cover sheet marked 'NHS – Confidential' must be included with any fax. **The cover sheet must include:**

- The name of the intended recipient.
- The name and contact details of the sender.
- Number of pages including the cover sheet.
- Has clear indication of how to contact the sender should the fax be received in error.

5.7.4. Regular recipients, pre –program the fax number where possible to minimise the risk of misdialling. The fax will be sent to a safe location where only staff that have a legitimate right to view the information can access it.

5.7.5. Staff must notify the recipient before sending the fax and ask for confirmation of receipt. This should be recorded on the fax cover sheet. Exceptionally, where it is essential to send a fax out of hours, this may occur where the sender is both confident that the destination fax number is current and that the fax machine is located in a secure, access-controlled environment. Confirmation of receipt will need to be sought during office hours.

5.7.6. Take care to dial the correct number.

5.7.7. Confidential faxes must not be left unsecured for unauthorised staff to see.

5.7.8. Only the minimum amount of personal information must be sent, where possible the data must be anonymised or a unique identifier used.

5.7.9. Faxes sent must include a front sheet, which contains a suitable confidentiality clause.

5.8. Communications by Post

5.8.1. All sensitive records must be stored face down in public areas and not left unsupervised at any time.

5.8.2. Incoming mail must be opened away from public areas.

5.8.3. Outgoing mail (both internal and external) must be sealed securely and marked 'private and confidential'. Where the contents are particularly sensitive or multiple records are included, 'Special Delivery' or an approved courier service must be used.

5.8.4. Return address details must also be provided should the item be undeliverable.

5.9. Computers / iPads / Laptops

5.9.1. Access to any PC / Trust issued iPad / Laptops must be password protected and passwords must never be shared. Passwords must be strong and in line with the Trust password naming convention (one that contains a mixture of upper and lower case letters; numbers and symbols).

5.9.2. Computer screens must be positioned so that they cannot be viewed by members of the general public or staff who do not have a justified need to view the information.

5.9.3. PCs, laptops and iPads when not in use must be switched off, locked, logged off the network or have a secure screen saver device in use.

5.9.4. Confidential or PID must only be saved on the Trust's network drives, never on your local hard drive or desktop.

5.9.5. The drive you choose will depend on the 'need to know' principle. Consider who needs to access the information that you save before choosing the location as follows:

'T' (Team) drive	Accessible by all members of your team/department – may be appropriate for some PID
OneDrive	This is part of Office 365 and is a personal storage facility.

5.9.6. **Mobile devices**: Patient data must only be saved on a Trust approved device issued by the Trust's IT department which is appropriately encrypted.

5.9.7. Whilst the Trust does allow personal devices to be used, under **NO** circumstances should personal non Trust equipment be used to store patient / employee / Trust information.

5.9.8. **Internal email**: Confidential business or personal information may be sent internally where both the sender and recipient have a Trust email address (i.e. from fred.bloggs@secamb.nhs.uk to joe.bloggs@secamb.nhs.uk).

5.9.9. However, only the minimum data must be used. For example, initials accompanied by an incident number.

5.9.10. Care must always be taken when using email. Even with careful use this does however carry some degree of risk.

5.9.11. **Therefore, before sending an email always ensure that:**

5.9.12. You select the correct recipient – care must be taken in instances where there is more than one individual with the same name.

5.9.13. Email uses an 'auto populate' function so care must be taken to ensure that the recipient details are correct.

5.9.14. The correct document is attached. **ALWAYS** double check attachment prior to sending an email.

5.9.15. You use minimal information in emails. For example, use initials instead of full names wherever possible.

5.9.16. When sending patient / personal information that a secure method of email is used. Example nhs.net to nhs.net.

5.9.17. Remember ALL emails and Skype / MS Teams for business communications are disclosable.

5.9.18. **Email within the NHS**: All Trust email communication will be via the the Trust's email (@secamb.NHS.UK). The Trust is accredited by NHSD as being secure (Secure email standard - DCB1596) and all confidential or personal information will be sent by this method. **The use of personal email accounts for transacting Trust communication is forbidden.**

5.9.19. **The following recipients will be regarded as being email addresses within the NHS:**

- **SECAmb** (*.SECAmb.NHS.UK)
- **NHSmail** (*.nhs.net)
- **xGSI** (*.x.gsi.gov.uk)
- **GSI** (*.gsi.gov.uk)
- **GSE** (*.gse.gov.uk)
- **GSX** (*.gsx.gov.uk)

- **CJX** (*.police.uk *.pnn.police.uk *.cjsm.net)
- **SCN** (*.scn.gov.uk)
- **GCSX** (*.gcsx.gov.uk)

5.9.20. Please refer to the attached link for national guidance around secure email: https://digital.nhs.uk/services/nhsmail/the-secure-email-standard#list-of-accredited-organisations

5.9.21. **Internet Email**: Due to its insecure nature, any information transmitted over the internet has to be regarded as being placed in the public domain.

5.9.22. Under no circumstances must confidential or personal information be sent to or from an internet email account (e.g. hotmail, yahoo etc.).

5.9.23. All staff must also read the Trust's Internet and Email policy for more guidance on sending of personal information electronically.

5.9.24. Guidance for Sharing Personal information by Phone, Post and Fax plus Transporting can be found in Appendices 2-5.

6. Responsibilities

6.1. The Chief Executive Officer is ultimately responsible for security and patient confidentiality. However, responsibility for the safe transfer of patient information is delegated to the Medical Director who is the Trust's Caldicott Guardian.

6.2. The Executive Director of Strategy and Business Development is the Trust's Senior Information Risk Owner (SIRO) who has specific responsibility for managing information security risk within the Trust.

6.3. Information Asset Owners (IAOs) are responsible for the security of information systems and assets within their control. They are supported by Information Asset Administrators.

6.4. The Head of Information Governance / IG Manager will monitor adherence to this policy, investigate breaches and provide guidance to staff.

6.5. Responsibility for compliance with this policy and guidance rests with individual directors and managers to:

- Ensure that Safe Havens are secure.
- Authorise access to appropriate staff.
- Ensure staff have access to relevant procedures.
- All staff have a responsibility to adhere to this policy and guidance.

7. Competence

7.1. All staff are required to undertake mandatory annual information governance training in accordance with training needs analysis. Information Governance training also forms part of the induction for new staff.

8. Monitoring

8.1. Compliance with this policy and guidance will be monitored by the Information Governance Working Group which will review incidents, near misses and risks raised through the Incident Reporting Procedure (DIF -1 process).

9. Audit and Review

9.1. This document will be reviewed at least every two years or sooner should there be changes in legislation, national guidance or working practices that warrant an earlier review.

9.2. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

9.3. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

9.4. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

10. References

- Data Protection Act 2018
- UK General Data Protection Regulation
- Human Rights Act 1998
- NHS Digital - https://digital.nhs.uk
- Confidentiality: NHS Code of Practice 2003
- NHSx Records Management Code of Practice 2021

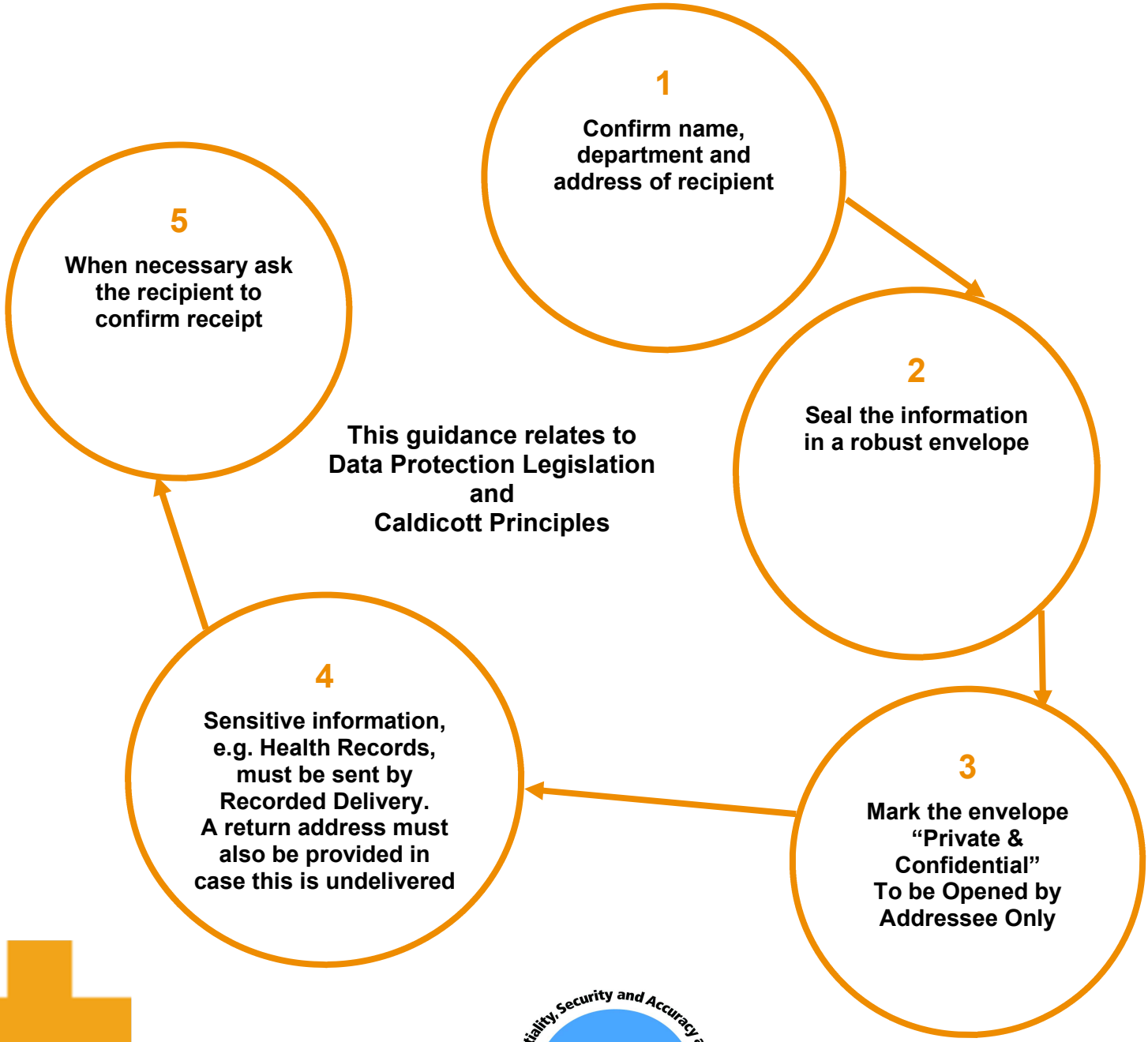
- Information Security Management: NHS Code of Practice, 2007
- Caldicott Standards into Social Care – Department of Health
- https://digital.nhs.uk/services/organisation-data-service/file-downloads/safe-haven-directory

11. Appendix 1

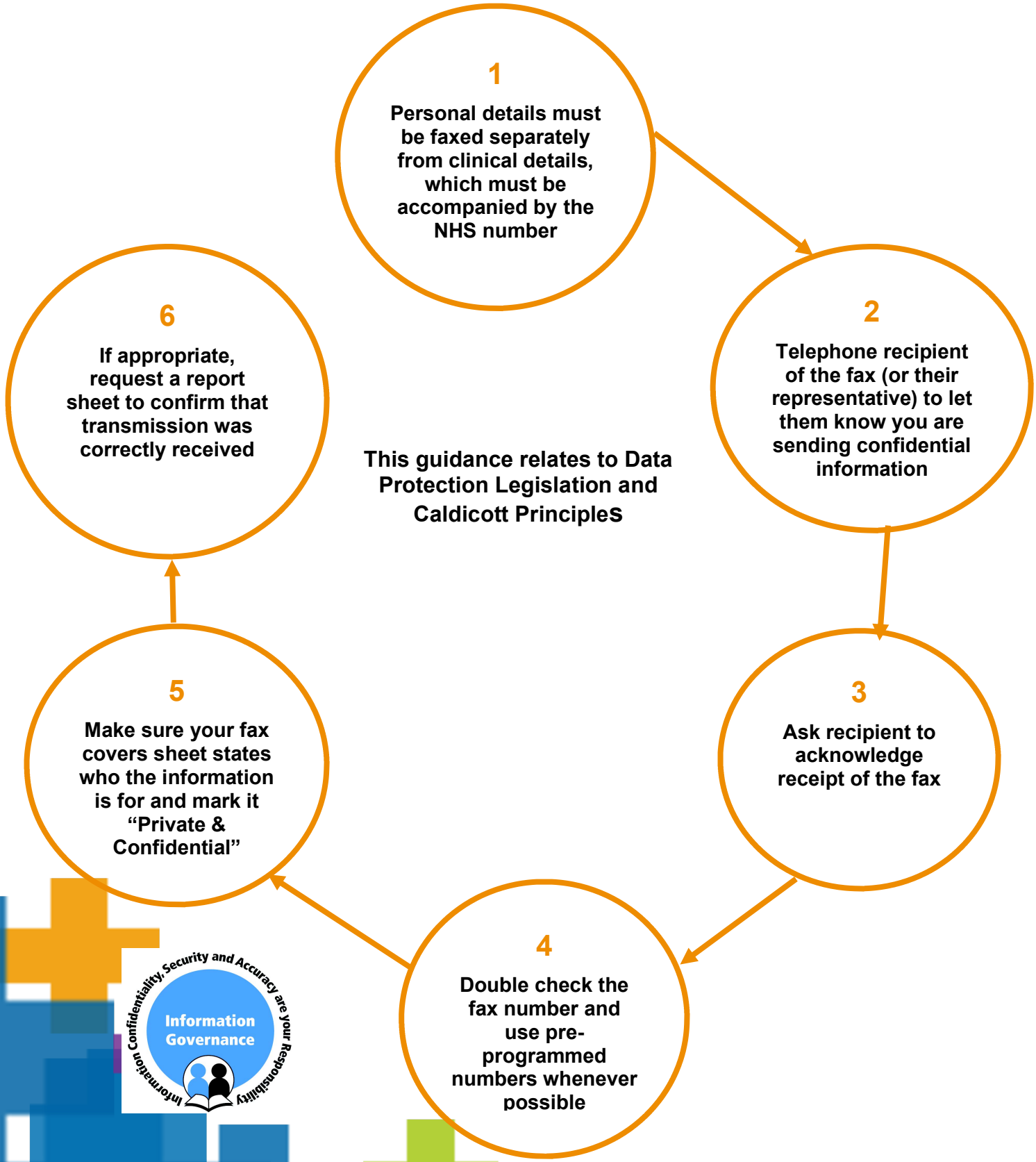
Guidance for Sharing Personal Information by Phone

12. Appendix 2

Guidance for Sharing Personal Information by Post



13. Appendix 3 Guidance for Sharing Personal information by FaxThis method must only be used in exceptional circumstances



14. **Appendix 4** Guidance for Transporting Personal Information

1
Person identifiable information must only be taken off site when absolutely necessary, or in accordance with local policy

2
Record what information you are taking off site, the reasons and if applicable where and to whom you are taking it

3
Information must be transported in a sealed container

4
Never leave personal identifiable information unattended. This must be retained in a 'safe haven', secure area

5
Ensure the information is returned back on site as soon as possible

6
Record that the information has been returned

This guidance relates to Data Protection Legislation And Caldicott Principles 4 and 6

Information Governance – Information Confidentiality, Security and Accuracy are your Responsibility