Bolton Clinical Commissioning Group

# Secure Transfer of Information Guidance

| | |
|---|---|
| **Policy Number** | **IG012** |
| **Target Audience** | **CCG and CSU staff** |
| **Approving Committee** | **CCG Executive** |
| **Date Approved** | **June 2015** |
| **Last Review Date** | **June 2015** |
| **Next Review Date** | **June 2017** |
| **Policy Author** | **Senior IG Officer (CSU)** |
| **Version Number** | **V2.0** |

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

## Version Control Sheet

| Version | Date | Reviewed By | Comment |
|---|---|---|---|
| 0.1 | Sept 13 | G Birch<br>M Robinson<br>D Sankey | Progress to CCG Executive for approval |
| 1 | September 2013 | CCG Exec | Approved |
| 1.1 | June 2015 | IG Team | Reviewed & progress to IM & T Operations Board for approval. |
| 2.0 | June 2015 | IM & T Operations Board | Approved |
| | | | |

| | | |
|---|---|---|
| Analysis of Effect completed: | By: M Robinson | Date: Sept 2013 |

Contents Page

## 1. Introduction and Aims

**1.1.** The purpose of this document is to provide guidance to all Bolton CCG staff on the secure transfer of information.

**1.2.** A number of Acts and guidance dictate the need for safe haven arrangements to be set in place, they include (but are not restricted to):

- **Data Protection Act 1998** (namely Principle 7): "Appropriate technical and organisational measures shall be taken to make personal data secure"

- **NHS Code of Practice: Confidentiality** (namely Annex A1 Protect patient Information) "Care must be taken, particularly with confidential clinical information , to ensure that the means of transferring from one location to another are secure as they can be"

All CCG staff must maintain the confidentiality of personal confidential data when both using it and transmitting.

Where the term Safe Haven is used, it refers to a location (or in some cases a piece of equipment such as a fax machine) situated on CCG premises where arrangements and procedures are in place to ensure sensitive or confidential information can be held, received and communicated securely

**1.3.** Depending on the content of information being sent Safe Haven procedures should be applied when it is of a Personal/Sensitive/Confidential nature**.**

**1.4.** When information is being transferred from one CCG/location/organisation to another, staff need to be confident of the safety and security of how the information is being transmitted.

**1.5.** This document sets out a framework within which staff responsible for all routine flows of personal confidential data, personal staff information and commercial in confidence information and any similar exchanges should adhere to. Any data flow must be between designated safe haven contact points. NHS staff use a wide variety of methods of handling and transferring confidential information e.g.

- Fax Machines
- Answer phones
- Telephones
- Photocopiers
- Electronic Communication (Email)
- Message Books/Boards
- Post
- Visitors Books
- Dictation Machines
- Removable Media
- Bulk data transfers

**1.6.** This guidance is designed to protect the CCG as an organisation, its constituent businesses and staff by defining the use and application of encryption technology when accessing, storing and transmitting CCG corporate, personal or patient

information.

### 1.7. Health and Social Care Act (2012)

Primary Care Trusts (PCTs) were abolished on 31 March 2013 and Clinical Commissioning Groups (CCGs) were established from 1 April 2013 with the majority of the responsibilities from PCTs. However, **CCGs are not direct successors of PCTs and do not have the legal rights to process Personal Confidential Data (PCD), for secondary uses that PCTs had**. The Health and Social Care Act 2012 states that only the Health and Social Care Information Centre (HSCIC) is able to receive and process PCD, for secondary use, without patient consent.

The Northwest Data Management and Integration Centre (DMIC) currently act as a regional office for the HSCIC and are able to process PCD legally.

NHS England has received a Section 251 exemption which allows limited data flows from DMIC to Accredited Safe Havens (ASH) to support some specific commissioning purposes.

**What can the CSU do now?**
Provide PCD to CCGs for use in GP clinical dashboards (includes risk stratification) if the following conditions are met:

- The only users that can see PCD are clinicians - viewing their own patients
- The data is supplied via the DMIC staff seconded to the HSCIC
- CCG staff do not have any direct interaction with PCD used by the system
- The systems uses role-based access control (RBAC)

Provide centralised Service Level Agreement Monitoring (SLAM) which includes:

- Centralised patient registration challenges
- Pseudonymisation of SLAM information for finance, contracting, Business Intelligence and Provider Management teams

To provide assurance to the DMIC and HSCIC that the conditions above are in place, CCGs will be required to provide details around the security and governance processes in place and sign a DMIC Data Sharing Contract.

**What does this mean for CCGs?**
**CCGs cannot:**

- send or receive PCD directly from care providers or any other sources for commissioning purposes
- validate Non Contract Activity
- validate activity charged for by Trusts
- use PCD for risk stratification, (unless ASH status achieved). However the DMIC can access or process historic/legacy PCD

**CCGs can:**

- receive aggregated or pseudonymised data

The above should be considered in conjunction with all the following elements of this guidance.

## 2. Scope

**2.1.** This guidance applies to those members of staff who are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

**2.2.** This guidance relates specifically to the handling of personal confidential data both clinical and non-clinical that has been received, created, maintained, stored or destroyed by staff by the CCG (refer to Paragraph 1.7).

**2.3.** This guidance aims to raise awareness and provide guidance on:

- The legislation and guidance which dictates the need for a safe haven
- A definition of the term safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a safe haven environment

## 3. Definitions

**3.1. Person Identifiable information, now known as Personal Confidential Data (PCD)**

Personal Confidential Information (PCD) is information about a person which would enable that person's identity to be established by one means or another. This might be fairly explicit such as an unusual surname or isolated postcode or bits of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

**3.2. Sensitive Personal Information**

Sensitive personal information is a category of personal information that is usually held in confidence and whose loss, misdirection or loss of integrity could impact adversely on individuals, the organisation or on the wider community, for example, where the personal information contains details of the individual's:

- Health of physical condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Trade union
- Political opinions
- Criminal convictions

For this type of information even more stringent measures should be employed to ensure that data remains secure.

**3.3. Business Sensitive information**

This is information that if disclosed could harm or damage the reputation or image of an organisation.

**3.4.** **Safe Haven** – The term safe haven is term used to explain either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure personal confidential data is communicated safely and securely. It is a safeguard for confidential information which enters or leaves the organisation whether this is by fax, post or other means. Any members of staff handling confidential information, whether paper based or electronic, must adhere to the safe haven principles.

This term was initially meant to describe the transfer of fax messages, but should now cover the data held and used within

- Fax machines
- Telephones/answer phones
- Photocopiers
- Emails
- White boards/notice boards
- Manual records and books
- Post
- Dictation Machines
- Removable Media
- Bulk data transfers

## 4. Accountability, Responsibilities and Training

**4.1.** The Chief Officer who has overall responsibility for the implementations of the provisions of this procedure. As the Accountable Officer, they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

**4.2.** The CCG Caldicott Guardian has responsibility for ensuring Safe Haven procedures are in place throughout the organisation. The Governance and Risk Department will instigate and monitor an investigation if a breach of safe haven occurs.

**4.3.** Associate Directors/Line Managers have responsibility for ensuring that all staff are aware of safe haven procedures and to report any new flows in or out of the department/team/service/location or installation of communication modes such as a new fax machine, to the CSU Information Governance Lead.

**4.4.** All staff have a responsibility for ensuring the information is handled, used, stored and shared confidentially and appropriately. If in doubt individuals should seek guidance from their line manager in the first instance, or the CSU Information Governance Lead.

**4.5.** Staff will receive instruction and direction on this guidance from a number of sources.

- Policy/strategy and procedure manuals
- Line Manager
- Specific Training Course
- Other communication methods (Staff Briefing, Team Meetings)
- CCG Intranet

## 5. Location/Security Arrangements for a good Safe Haven Environment

**5.1.** Safe haven procedures should be in place in any location where confidential data is being received, held or communicated especially where the data is person identifiable.

**5.2.** When choosing a safe haven location the follow factors must be considered:

- A safe haven location must be a room that is locked or accessible via a coded key pad (or similar device) known only to authorised staff
- The office or workspace must be sited in such a way that only authorised staff can enter that location
- If sited on the ground floor any windows must have locks on them
- The room must conform to health and safety requirements in terms of fire safety from flood, theft or environmental damage
- Manual paper records containing personal confidential data must be store in locked cabinets when not in use and when the office/workstation is left unattended
- Operate a Clear Desk Policy, e.g. lock documents away if away from desk during the day, evenings and weekends
- Documents should not be left unattended for any significant period of time e.g. faxes should be collected/distributed from the fax machine at frequent periods and post should not be left unattended in pigeon holes or desks
- Computers must not be left on view or accessible to unauthorised staff and must have a secure screen saver function and be switched off when not in use
- Equipment such as fax machines in the safe haven must have a code password or pin and be turned off out of office hours

## 6. Data Transmission Processes

### 6.1. Transmission of Personal Information via Fax

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. Safe haven fax machines must be placed in a secure location and are lockable when unattended. Ideally they should require a code password or pin for operation and numbers for these dedicated fax machines must be made known. The following rules also apply:

- Clarify with the receiver that they operate safe haven procedures
- The fax is sent to a location where only staff that have a legitimate right to view the information can access it
- The sender is certain that the correct person will receive it and that the fax number is correct (always confirm with the receiving party before any information is sent)
- You notify the recipient when you are sending the fax and ask them to acknowledge receipt of the information and number of indicated pages
- Care should be taken in dialling the correct number. Frequently used numbers should be pre-programmed to reduce misdialling. Pre-programmed numbers should be routinely checked for accuracy
- Confidential faxes are not left lying around for unauthorised staff/members of the public to see
- Only the minimum amount of personal information should be sent. Where possible, the data should be anonymised or NHS Number unique identifier

used. Where both clinical and personal data is essential to be sent, you should consider sending them separately, ensuring the first fax has been received prior to sending the remainder

- Faxes sent should include a CCG front sheet which states 'Private and Confidential' and which contains the CCG confidentiality and disclaimer clause. The intended recipient's name and job title or department should be clearly included. Do not include any sensitive information on the front sheet
- A 'sent report' should be obtained which is evidence that the fax was sent to the correct fax number and received by the fax at the other end. This report should be kept secure as part of an audit trail
- Never leave the information unattended whilst it is being transmitted
- Do not send a fax to a destination where you know it is not going to be seen for some time or outside office opening times (whenever possible)

**Appendix A** displays a flowchart which can be printed, laminated and placed by a fax machine for reference.

### 6.2. Transmission of Personal Information via Computer and Email:

- Access to any PC must be password protected and passwords must **not** be shared
- Computer screens must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data. PCs or laptops not in use should be switched off or have a secure screen saver device in use
- Information must be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures
- The only accredited and secure way of transmitting patient-identifiable data by e-mail is via NHS Mail between NHS Mail accounts for NHS users. As long as both sender and recipient have the suffix @nhs.net, i.e. (firstname.secondname@nhs.net) emails will be sent/received via encrypted mail service. Refer to Paragraph 5 of Bolton CCG's Acceptable Use Policy Ref IG004 for further details on secure emailing and for a list of other non NHS domains for secure encrypted email transmission.
- To maintain confidentiality of data, outside third party organisations that do not have NHS Mail should have approved encryption software (AES) and a password has to be set which must consist of 8 characters long with a combination of numbers and letters. The password should be supplied by telephone to the recipient, and not issued in a separate email. Alternatively, documents emailed to the CCG may be password protected.
- All emails issued by CCG staff should include the standard disclaimer notice.
- Personal information of a more sensitive nature must be sent over NHS Mail with appropriate safeguards:
  - Emails which contain sensitive information should be appropriately titled i.e. do not include sensitive details in the subject line
  - Clinical information is clearly marked
  - E-mails are sent to the right people
  - Browsers are safely set up so that, for example, passwords are not saved and temporary internet files are deleted on exit
  - The receiver is ready to handle the information in the right way

### 6.3. Information Disclosure of Information by Telephone

There will be occasions when telephone enquiries are received asking for disclosure of personal information. When the disclosure is legally justified and

the caller has a legal right to access that information, the following rules should be adhered to:

- Verify personal details
- Obtain and record enquiries telephone number
- If the caller is part of an organisation/company, the main switchboard number of that organisation (via phone book or directory enquiries) should be obtained and ring back
- Conduct the call in area that is private where staff/public cannot overhear
- Any notes made during the calls should be kept in a secure place (locked away) and not left on any desk
- Any suspect bogus enquiries should be referred immediately to the CCG Information Governance Lead as soon as possible and an incident form completed
- Always provide the minimum amount of information that is necessary
- If in doubt, the caller should be advised that they will be called back, where necessary, a senior manager or the designated authority for confidentiality issues should be consulted
- Be aware of any press enquiries and refer to the relevant department within the CCG

**Appendix B** displays a flowchart which can be printed, laminated and placed by telephones for reference.

### 6.4. Communications by Post

**Incoming:**

- Ensure incoming post is received in an environment away from public interference e.g. not left on receptionist's desk in a waiting area
- Open incoming mail away from public areas
- Ensure if post is sorted for onward distribution that it is stored securely and is picked up frequently

**Outgoing:**

- Always double check addresses
- Mark post clearly with names and addresses and with 'Private and Confidential'
- Use a CCG letter headed front page or compliment slip
- Use a secure robust envelope, include a return address where appropriate
- For important letters/parcels, ask for confirmation of safe arrival
- Outgoing sensitive information should be protected from data loss in line with Department of Health guidance, by using a trackable service, i.e. Royal Mail Special Delivery or the CCG's authorised courier. Royal Mail Recorded Delivery is not a trackable service.

**Appendix C** displays a flowchart which can be printed, laminated and placed near staff who are more likely to handle incoming and outgoing post.

### 6.5. Communications by Text Message

Text messaging is becoming increasingly popular however there are potential information security risks that should be considered before any text messages are used. For example:

- Check the mobile number is correct and be confident that the person using the recipients mobile is the person to whom the message is intended
- Check that the patient has received the message
- Text messages are normally stored on SIM cards and are typically only cleared when overwritten (not necessarily when erased) – as mobile phones

are easy to misplace or may get stolen there is a danger of a breach of confidentiality occurring that the patient may find embarrassing or damaging
- Mobile phone networks may be open to additional risks of eaves dropping or interception

When using this method of communication minimum amount of confidential data should be sent. And remember that appropriate informed consent must have been sought prior to commencing text messaging communications.

### 6.6. Transfer of Paper/Hardcopy Documents

Paper records/documents may be required for investigation or to refer to as part of patients care. Care must be taken when transferring documents that contain confidential information:

- Paper documents that contain confidential information must be stored in a lockable cupboard or cabinet
- Lockable crates must be used to move bulk hardcopy information
- Only take off site when absolutely necessary, or in accordance with local policy
- Record what information is taken off site/from a department, and if applicable, where and whom the information has gone to
- Ensure documents are properly 'booked out' of any relevant filing
- Never leave personal/sensitive/confidential records/documents unattended
- Ensure the information is returned as soon as possible
- Record that the information has been returned

For further information on transferring paper documentation please refer to the CCGs Records Management Policy IG005.

**Appendix D** displays a flowchart which can be printed, laminated and placed near members of staff who work in/around paper records/documents containing personal confidential data and who may be asked to arrange transfer of the records.

### 6.7. Other Electronic Media

- Dictation machines and tapes can contain extremely sensitive information and should always be kept in a locked area when not in use. They should be cleared of all dictation when the communication has been completed
- Answer phones receiving personal information must have the volume lowered so that the information is not being un-necessarily overheard
- Photocopying machines should be sited in areas where the general public do not have physical access. No papers should be left on the glass after copying, *Always Check*.

## 7. Sharing information with non NHS organisations

**7.1.** Staff should be aware of the Data Sharing Processor Agreement and the requirement to have an Information Sharing Agreement in place for the routine sharing of personal confidential data.

**7.2.** Staff authorised to share/disclose personal information to other organisations outside the NHS must seek assurance that these organisations have a designated safe haven point for receiving personal confidential data.

**7.3.** The CCG must be assured that these organisations are able to comply with the safe haven ethos and that they meet certain legislative and related guidance:

- Data Protection Act 1998

- Common law duty of confidence
- NHS Code of Practice: Confidentiality

## 8. Monitoring and review

**8.1.** Performance against Key Performance Indicators will be reviewed on an annual basis and used to inform the development of future procedural documents.

**8.2.** This policy will be reviewed on an annual basis, and in accordance with the following as and when required:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities
- Changes to CCG organisations structure

## 9. Legislation and related documents

**9.1.** This policy and a set of procedural document manuals are available on the CCG Intranet.

**9.2.** A number of other policies are related to this policy and all employees should be aware of the full range below:

- IG001 Information Governance Policy
- IG002 Confidentiality and Data Protection Policy
- IG003 Corporate Information Security Policy
- IG004 Acceptable Use Policy (IT, Email and Internet)
- IG005 Records Management Policy
- IG006 Information Risk Policy
- IG007 Information Governance Incident Reporting Procedure
- IG008 Encryption Policy
- IG009 Confidentiality Audit Procedure
- IG012 Secure Transfer of Information Guidance

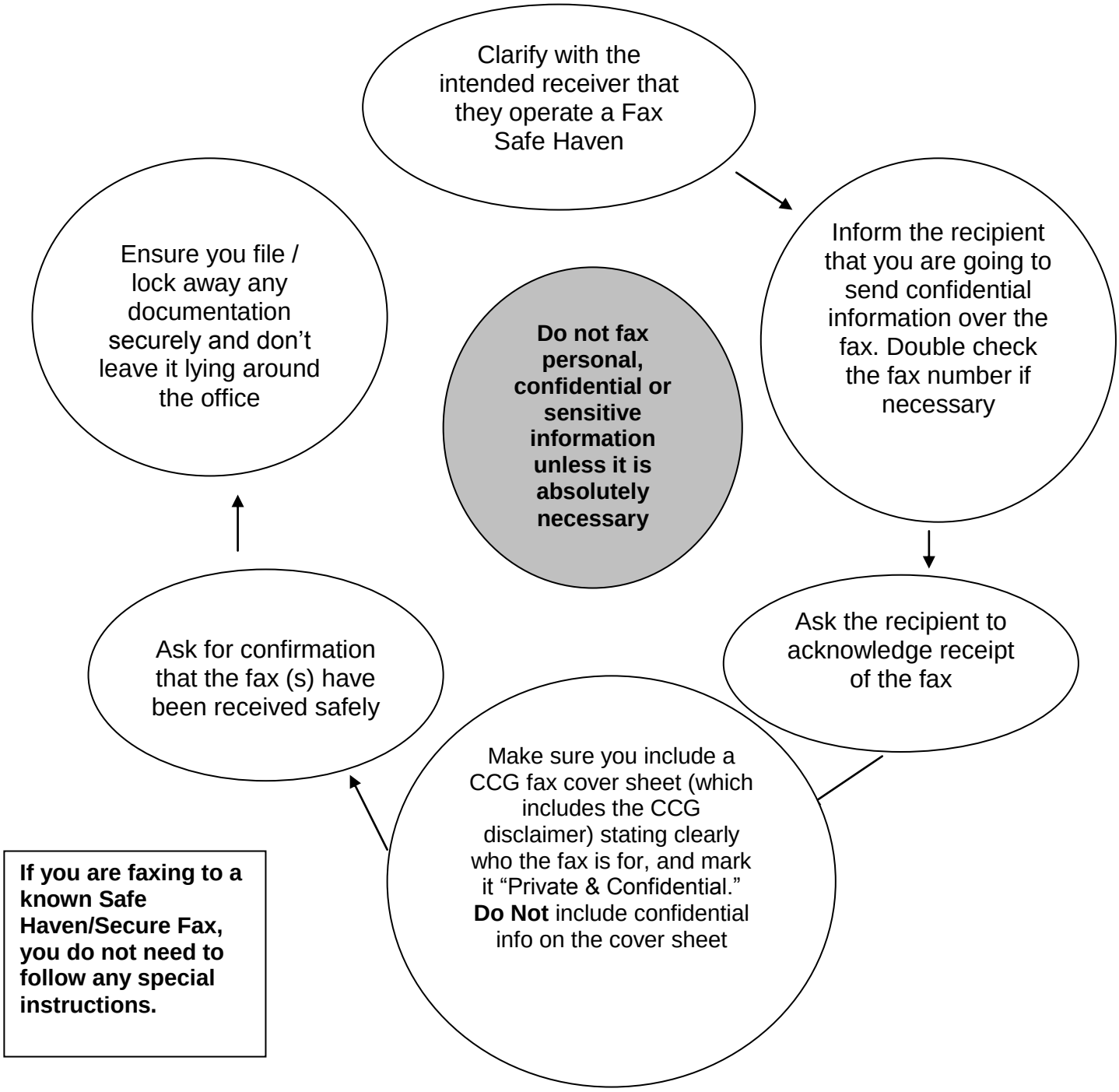
**9.3.** Acts Covered Under Policy

- Data Protection Act 1998
- Human Rights Act 1998
- Computer Misuse 1998
- Electronic Communications Act 2000

**9.4.** The CCG will also take action to comply with any new legislation affecting Safe Haven procedures as it arises.

Appendix A

# Guidance for sending Personal, Confidential or Sensitive information by FAX



Appendix B

# Guidance for sharing Personal, Confidential or Sensitive information by PHONE

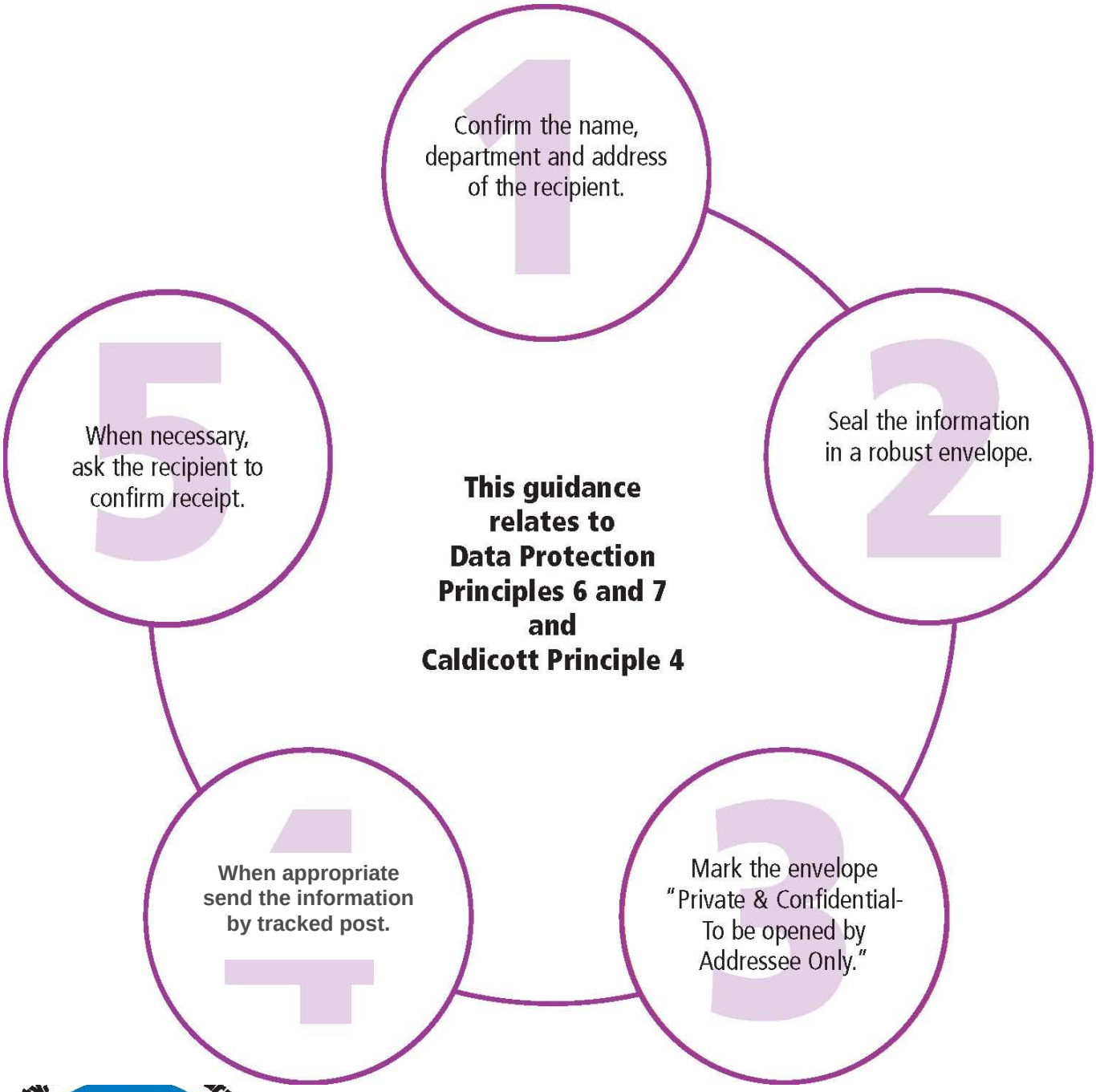




tio With acknowledgements to Surrey Health Community

Appendix C

# Guidance for sharing Personal, Confidential or Sensitive information by POST



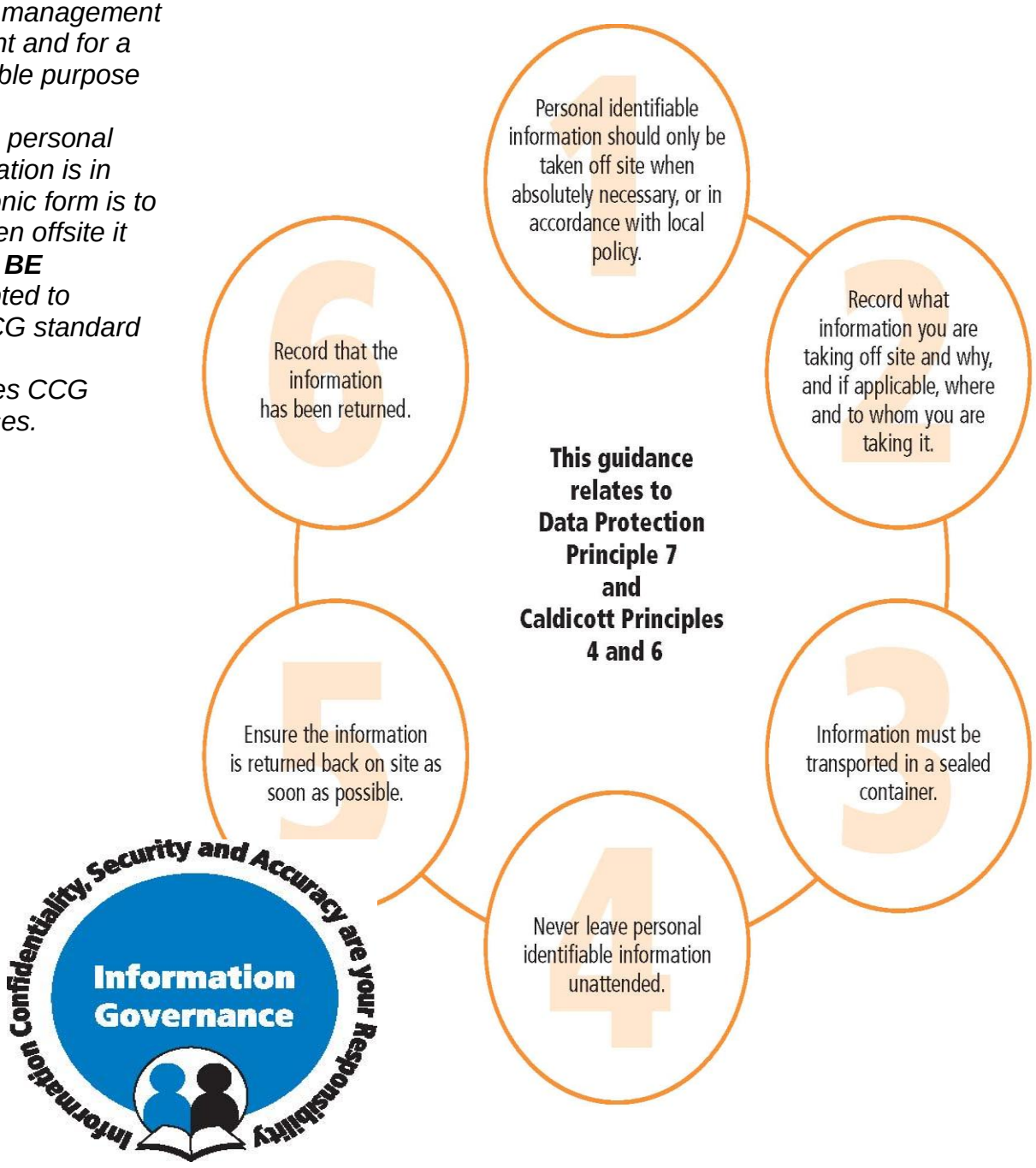
With acknowledgements to Surrey Health Community

Appendix D

*Personal information should not be taken offsite without explicit senior management consent and for a justifiable purpose*

*Where personal information is in electronic form is to be taken offsite it* ***MUST BE*** *encrypted to the CCG standard before it leaves CCG premises.*

# Guidance for TRANSPORTING for personal information off site



With acknowledgements to Surrey Health Community