Cambridgeshire and Peterborough
Clinical Commissioning Group (CCG)

SAFE HAVEN POLICY
2017 - 2019

Approval Process

Lead Author:	Information Governance Manager
Reviewed by:	Cambridgeshire and Peterborough CCG Information Governance, Business Intelligence and IM&T Group
Approved by:	Cambridgeshire and Peterborough CCG Information Governance, Business Intelligence and IM&T Group
Ratified by:	Clinical Executive Committee
Date ratified:	August 2017
Version:	3.0
Review date:	August 2019 (or earlier if significant change to local or national requirements)
Valid on:	August 2017

Document Control Sheet

Development and Consultation:	Policy developed by CCG Corporate Services Manager, in consultation with the IG, BI & IM&T Group and endorsed by CEC.
Dissemination	This policy will be promoted and available to all staff within the CCG.
Implementation	The Director of Corporate Affairs (SIRO) is responsible for monitoring the application of the policy by ensuring that:- • The policy is brought to the attention of all employees and building users • Managers are aware of their responsibilities for ensuring that staff under their control implement and adhere to the policy • Staff are informed and consulted as appropriate • Appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy.
Training	Training will be undertaken as part of the CCG's on-going processes.
Audit	Implementation of the Policy will be monitored in line with Information Governance Toolkit requirements
Review	This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation.
Links with other Documents	The Policy should be read in conjunction with: Information Governance Policy Information Sharing Framework Information Security for Staff Policy NHS Code of Confidentiality Code of Conduct for Confidentiality Records Management Policy Removable Media Policy Destruction and Disposal of Unwanted Information and Equipment Policy
Equality and Diversity	The Corporate Service Support Manager for Equality and Diversity (E&D) has carried out a Rapid E&D Impact assessment and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
1	Whole document	Development of policy for Cambridgeshire and Peterborough CCG	April 2013
1.1	Appendices 3 & 4	Fax header sheets amended	September 2013
1.2	Links with other Documents	Updated policy list	Nov 2013
2.0	Whole document	Reviewed and ratified by CMET	July 2015
3.0	Whole document	Business Intelligence inclusion, Information Sharing Protocol is now the county wide Information Sharing Framework, addition of 7th Caldicott Principle Addition of 2.2. Section 4 updated. Section 7.3 added	May 2017

Safe Haven Policy

Table of Contents

Safe Haven Policy

1. Purpose

1.1. All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of person identifiable information held. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information e.g. a person's medical condition.

1.2. Where Trusts and external partner agencies want to send person identifiable information to a CCG department, they should be confident that they are doing so to a location that maintains the security of the data.

2. Scope

2.1 This policy provides:

- The legislation and guidance that dictates the need for a safe haven.
- A definition of the term 'safe haven'.
- Outlines when a safe haven is required.
- The necessary procedures and requirements that are needed to implement a safe haven.
- Rules for different kinds of safe haven.
- Sets out access disclosure rules.

2.2 This policy applies to all CCG staff which for the purposes of this policy and includes but is not limited to governing body members, contractors, agency & temporary staff, student, honorary and volunteer staff. It is applicable to all areas of the CCG and adherence should be included in all contracts for commissioned or collaboratively commissioned services, without exception.

3. Legislation and guidance

3.1 A number of Acts and guidance dictate the need for safe haven arrangements to be set in place, they include:

Data Protection Act 1998 (Principle 7) '*Appropriate technical and organisational measures shall be taken to make person identifiable information secure.'*

NHS Digital Code of practice on confidential information – – Annex 1 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.'*

NHS Information Governance Toolkit requires the organisation to have a documented plan to ensure that transfers of person identifiable and sensitive information are adequately secure.

Caldicott Principles:

- Justify the purpose. Who is asking for the information? Why do they want it?
- Only use person identifiable information when it is absolutely necessary
- Use the minimum person identifiable information required
- Access should be on a strict ‘need to know’ basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

4. Definitions

4.1. **Safe haven** – The term safe haven is recognised throughout the NHS to describe the administrative arrangements to safeguard the confidential transfer of person identifiable information between organisations or sites. This term was initially meant to describe the transfer of facsimile messages, but should now cover the data held and used within:

- Fax machines
- Post
- Telephones/answer phones
- Digital and manual records and books
- White boards/notice boards
- Emails
- Bulk data transfers

4.2. **‘Person Identifiable’ information** - As per the Data Protection Act 1998: Personal data are data which relate to a living individual who can be identified
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.3. **‘Sensitive Person Identifiable’ information** – This is information that contains sensitive personal detail and is a subset of Personal Data.

Sensitive personal information is personal data consisting of information as to:
(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,
(d) whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) their physical or mental health or condition,
(f) their sexual life,
(g) the commission or alleged commission of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

4.4. **Confidential Personal Data**
This is personal and usually sensitive personal data that is held subject to an obligation of confidentiality. Clinical data relating to an identifiable individual is almost always confidential and some data recorded by social care staff may also be subject to this obligation.

4.5 **Business Sensitive information** – This is information that if disclosed could harm or damage the reputation or image of an organisation.

5. Identifying when safe haven procedures should be in place

5.1. Safe haven procedures should be in place in any location where large amounts of person identifiable information is received, held, or communicated, especially where the person identifiable information is of a sensitive nature.

5.2. There should be at least one area designated as a safe haven at each of the CCG sites.

6. Requirements for safe havens

6.1 Location / security arrangements:

- It should be in a room that is locked or accessible via a coded key pad known only to authorised staff, **OR**
- The office or workspace should be sited in such a way that only authorised staff can enter that location, i.e. it is not an area which is readily accessible to any member of staff who work in the same building or office, or any visitors.
- If sited on the ground floor any windows should have locks on them.
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage.
- Manual paper records containing person identifiable information should be stored in locked cabinets. Desks should be kept clear and all person identifiable data locked away at the end of the day.
- Computers should not be left on view or accessible to unauthorised staff and should have a secure screen saver function and be switched off when not in use.
- When installing fax machines in the safe haven consideration should be given to any security tools available on the machine, such as password protected memory. If the room containing the machine cannot be locked overnight, machines should be turned off out of office hours.

7. Rules for different kinds of safe haven

All points of receipt of information should be given safe haven consideration by staff: phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information, notice boards etc.

All staff should be alert to the need to protect confidential information should it come their way. For guidance on what can be shared and how, staff should refer to the Data Protection and Access to Records Policy and the Cambridgeshire and Peterborough Health and Social Care Information Sharing Framework or contact the IG team or Caldicott Guardian.

7.1 By Telephone

For incoming calls where person identifiable information is shared with someone unknown the following practice must be adhered:

- Confirm the name, job title, department and organisation of the person requesting information
- Confirm the reason for request, if appropriate
- Take a contact telephone number, e.g. main switchboard number
- Check whether the information can be provided. If in doubt tell the enquirer you will call them back
- Provide the information only to the person who has requested it (do not leave messages)
- Ensure that you record your name, the date and time of disclosure, the reason for it and who authorised sharing. Also record the recipient's named, job title, organisation and telephone number.
- Staff are expected to apply common sense with regard to the open plan office and use an available private room for telephone conversations that are highly confidential.

7.2 By Email

NHS mail is currently the only NHS approved method for exchanging person identifiable or sensitive data, but only if both the sender and recipient use an NHS mail account or if sending to another government secure domain.

Central Gov	**.gsi.gov.uk**	**.gse.gov.uk**	**.gsx.gov.uk**
	.mod.uk	**.pnn.police.uk**	.**scn.gov.uk**
	.cjsm.net		
Local Gov	**.gcsx.gov.uk**		

They should be stored appropriately on receipt. For example saved to the Restricted drive or details should be incorporated into the relevant database or health record and the original email should be deleted.

Please refer to the Information Security Staff Policy.

7.2.1 Email encryption

A new NHS mail encryption feature means that NHS mail users can also securely exchange sensitive information with users of non-accredited or non-secure email services, for example those ending in .nhs.uk, Hotmail, Gmail and Yahoo. The new NHS mail encryption feature means that health and social care staff now benefit from a secure service which allows them to communicate across organisation boundaries and industry sectors. NHS mail can now be used securely across the entire health and social care community – in fact with anyone using any email account.

With the new NHS mail encryption feature:

- NHS mail users can easily communicate securely with users of ANY email service including those ending .nhs.uk without having to manually encrypt sensitive information
- Users can send attachments which will automatically be encrypted for you and remain secure
- Organisations can save money by replacing existing post, fax and phone-based processes with secure email
- Users of non-accredited or non-secure email services can communicate securely with NHS mail users saving time and money, speeding up communications and improving patient care
- Communication is faster, easier and more reliable.

Full guidance can be obtained by the following link:
http://support.nhs.net/policyandguidance

For NHS mail users:
If you have a contact that uses a non-accredited or non-secure email service (e.g. ending .nhs.uk) with whom you need to exchange sensitive information, you will need to set up the communications channel with them first by sending the initial encrypted email that they can then open, read and reply to securely. Download the full step-by - step guidance for senders.

For non-NHS mail users:
In order to send an encrypted email to an NHS mail user, they must email you first. You can then reply to or forward their email and it will remain encrypted. You can also include attachments.

When you've received an encrypted email from an NHS mail user, in order to open it, read it and reply you will need to register for an account with the NHS mail encryption provider. Step-by-step instructions can be found in the guidance for recipients.

Users of the NHS mail email encryption service Note the following:

- Before you send an encrypted email, talk to the person you're sending it to – make sure that they're expecting the information and are ready to deal with it appropriately;
- It's your responsibility to safeguard any sensitive data you receive – if you are receiving the information on behalf of an organisation, you should do so in line with local data protection and information governance policies;
- If you are sending information to a patient, gain consent from them before you communicate with them via NHS mail and do so in line with your local information governance policies;
- Email delivery to Internet email addresses (e.g. Hotmail.com) can be unreliable. Sometimes messages are silently lost or sometimes a delivery notification is returned even if the message has not been received by the recipient. Where delivery assurance is required please ask the sender to reply to you confirming receipt.

7.3 **Fax machines**

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so and there is no alternative method. Outside of normal working hours, fax machines should either be turned off or be located in a locked office or cupboard.

7.3.1 The following rules must apply:

- The fax is sent to a safe 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.
- Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information
- Ask the recipient to acknowledge receipt of the fax.
- Care is taken in dialling the correct number and the number is checked before hitting the “send” button
- Confidential faxes must not be left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent, where possible the data should be anonymised or a unique identifier used.
- Faxes sent must include a cover sheet, which contains a suitable confidentiality clause and is marked ‘Private and Confidential’. (See Appendix 3 for template.)
- Personal details should be faxed separately from clinical details, which must be accompanied by the NHS number – do not fax personal or confidential information unless it is absolutely necessary. Confirmation of receipt should be sought before sending the second/subsequent data.
- If appropriate request a report sheet to confirm that transmission was complete.
- If you find a confidential document has been faxed to your machine, it is your responsibility to ensure that it is given to the named recipient and/or the sender has been notified of the error.

Fax guidance is available on the website and displayed by the fax machines

7.3. By Post

- All sensitive documents must be stored face down in public areas and not left unsupervised at any time.
- Recipients of frequent or significant numbers of confidential mail are advised to keep a log to record receipt and transfer within the organisation.
- Incoming mail should be opened away from public areas.
- Confirm the name, department and address for the recipient. Do not use acronyms as they can be easily confused.
- Outgoing mail (both internal and external) must be sealed securely and the envelope marked ‘Private and Confidential, Addressee only’.
- For highly sensitive information courier or special delivery should be used and signed confirmation of receipt obtained.
- In general consideration should be given to transit method and distance when choosing suitable secure packaging material.
- In all cases the addressee or recipient should acknowledge receipt of the information.
- Confirm receipt.

7.4. Transfer of confidential hardcopy information

- Lockable crates must be used to move bulk confidential hard copy information from one place to another. Hardcopy information must be stored in a locked cupboard or cabinet.
- Obtain a receipt for hand delivered confidential information.
- Person identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.
- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it.
- Information must be transported in a sealed container.
- Never leave person identifiable information unattended.
- Ensure the information is returned as soon as possible.
- Record that the information has been returned.

7.5. Use of Couriers and Taxis to transport confidential information

- Only companies that hold an existing service level agreement with the organisation with an appropriate confidentiality clause can be used to transport Trust patients, staff, equipment or documentation – advice should be sought from the Information Governance Team if the name and contact details of the company are not known.
  Any items for transport in this way should be signed in and out appropriately and copy evidence of sending/receipt retained

7.6. Transferring confidential information by removable media

Please refer to the *Removable Media Policy.*

8. Use of Computers

- Access to any computer must be password protected in line with current IT access rules; this password must not be shared.
- Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see person identifiable data. Press Control, Alt, and Delete together and choose option 'Lock Computer' to secure your computer when away from your desk. Computers or laptops not in use should be switched off or have a secure screen saver device in use.
- Information should be held on the organisation's network servers, and not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.
- Information should not be saved or copied into any PC or media that is "outside the NHS".
- Personal information should be sent over NHS mail with appropriate safeguards:
  - Clinical information is clearly marked
  - Emails 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

- Information sent by email will be safely stored and archived as well as being incorporated into patient records
- There is an audit trail to show who did what and when
- There are adequate fall back and fail-safe arrangements.

9. Safe haven printers

There are no designated safe haven printers, however, CCG sites with printers that have a ‘secure print’ function should use this to print confidential documents e.g. Multi-Functional Devices. Where this is not possible, staff must ensure confidential printing is collected immediately.
Confidential printing that is left lying around should be reported to the IG team.

10. Sharing information with non NHS organisations

10.1 Staff authorised to disclose information to other organisations outside the NHS must seek an assurance that these organisations have a designated safe haven point for receiving person identifiable information.

10.2 NHS Cambridgeshire and Peterborough CCG must be assured that these organisations are able to comply with the safe haven ethos and meet certain legislative and related guidance requirements:

- Data Protection Act 1998
- Common law duty of confidence
- NHS Digital Code of practice on confidential information

10.3 Staff sharing person identifiable information with other agencies should do so in compliance with the policies listed on the Document Control Sheet.

11 Roles & responsibilities

It is recognised that all staff in the organisation have responsibility for ensuring the safe receipt, maintenance and disclosure of person identifiable information and that it is done in line with this policy and that good practice is maintained throughout the organisation.

Caldicott Guardian is responsible for ensuring person identifiable information is received, stored and used in line with the Trust obligations to the Data Protection Act 1998 and the NHS Information Authority Information Governance Toolkit.

SIRO (Senior Information Risk Owner) is responsible for protecting data and managing information risks

Directors are responsible for ensuring CCG safe haven procedures are known and followed in their areas.

All CCG staff that process person identifiable information are responsible for ensuring safe haven guidance is adhered to.

Confidentiality breaches should be reported immediately to the line manager and Information Governance Team prior to entry onto the Datix system.

12 Monitoring and Assurance

12.1. The IG, BI and IM&T Committee will review Incident Reporting as a standing item on its agenda.

12.2. The SIRO will escalate information risks to the Governing Body.

12.3 There is an annual programme of internal and external audits in place which provides validation and assurance of the information governance systems.

12.4 NHS Cambridgeshire and Peterborough CCG use a complaints system to effectively respond to complaints in connection with the Data Protection Act and Information Governance.

12.5 IG training uptake is regularly reviewed by the CCG Clinical Executive Committee.

13 Equality & Diversity Impact Assessment

13.1 In reviewing this policy, NHS Cambridgeshire and Peterborough CCG has considered, as a minimum, the following questions:

- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so is this planned?

13.2. Adverse impact has been considered for age, disability, gender, race/ethnic origin, religion/belief/sexual orientation.

Appendix 1

Safe Haven faxes at Lockton House:

CCG Headquarters – Lockton House
Lockton House
Clarendon Rd
Cambridge
CB2 8FH

Complex Cases Team – Floor 4
Safe Haven Fax (01223) 725591

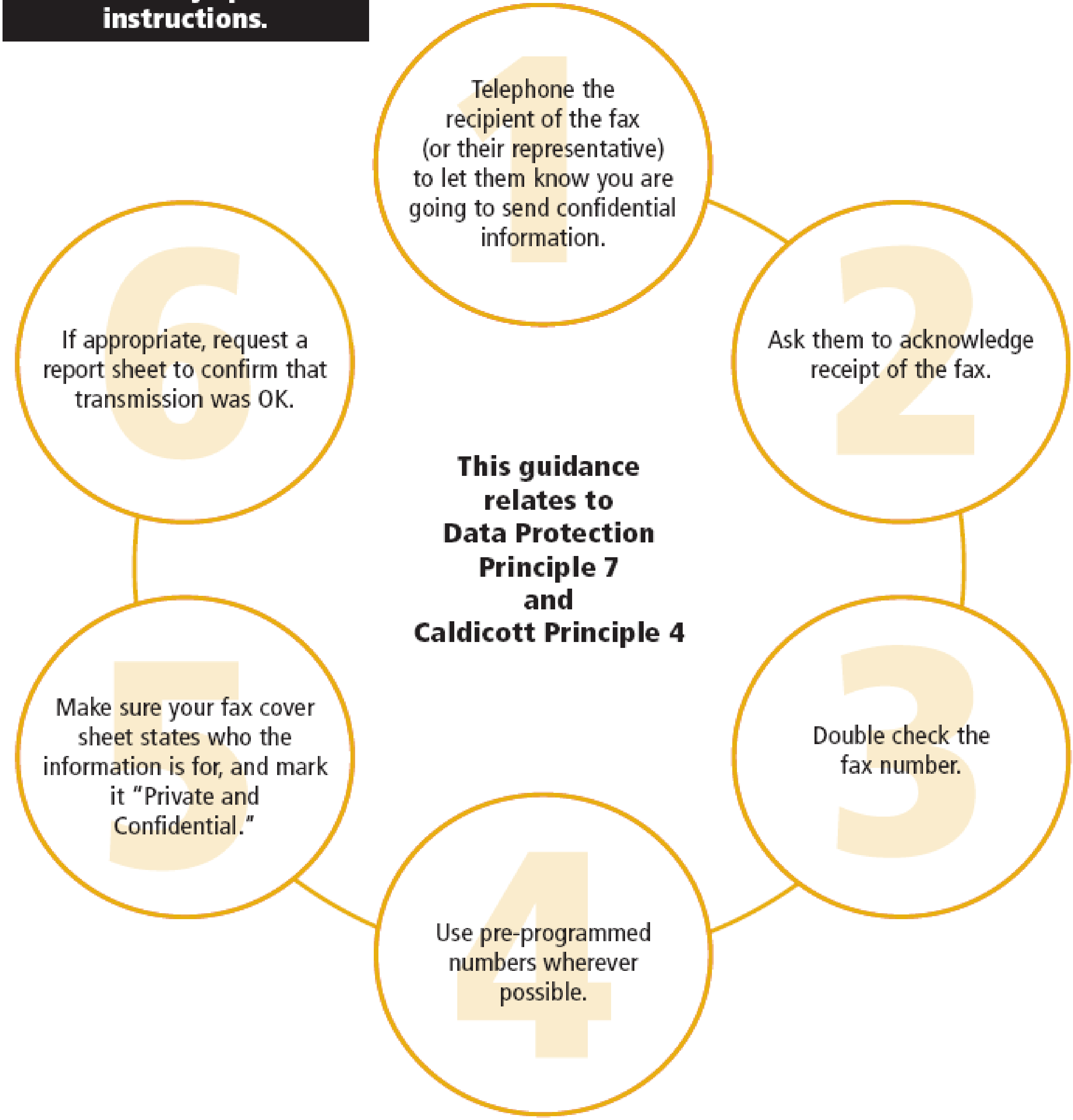
The CCG is in the process of phasing out the use of Fax machines

Appendix 2

Guidance for sharing person identifiable information by FAX

If you are faxing to a known Safe Haven/Secure Fax, you do not need to follow any special instructions.

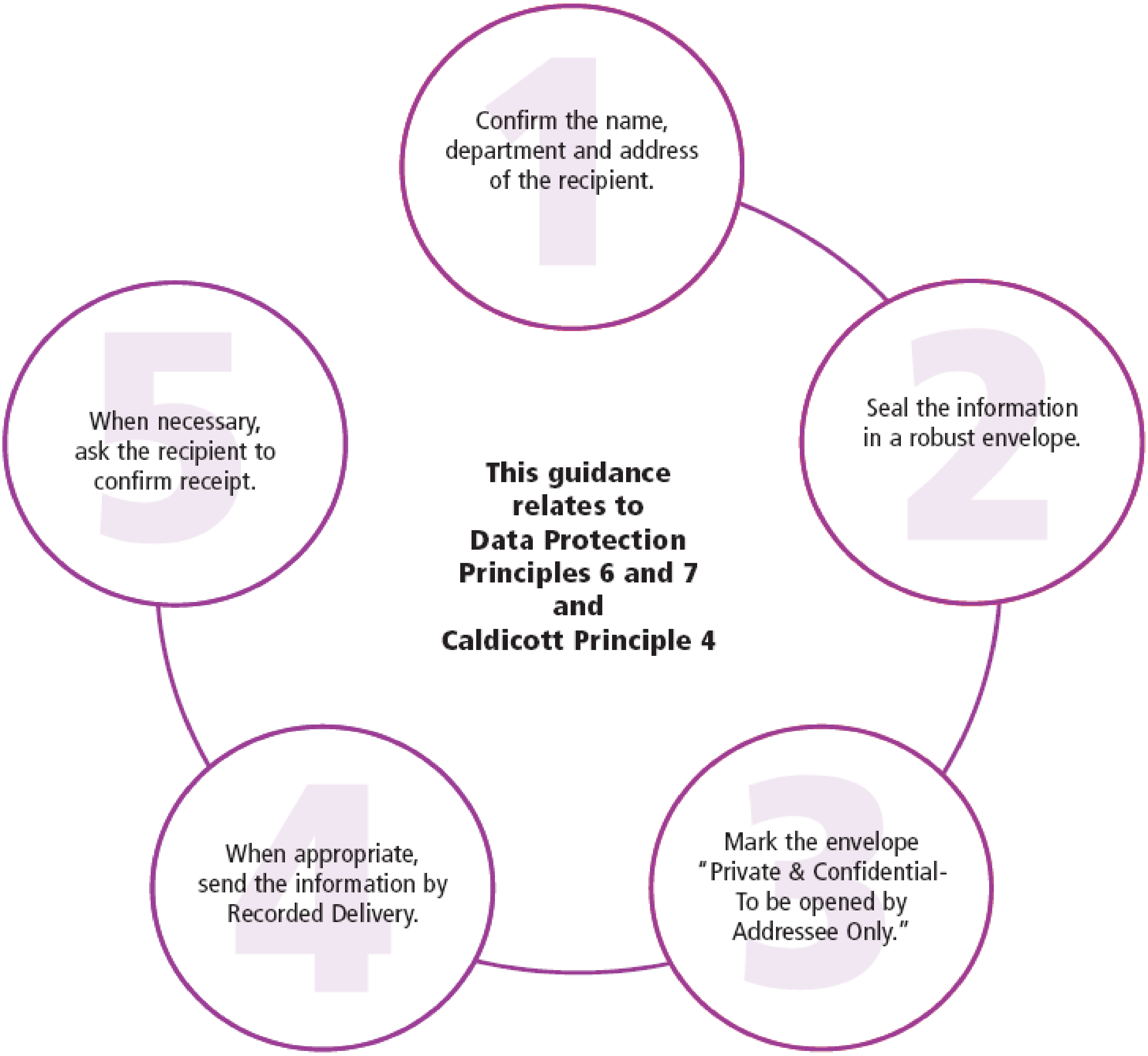
If not follow steps 1-6



1. Telephone the recipient of the fax (or their representative) to let them know you are going to send confidential information.
2. Ask them to acknowledge receipt of the fax.
3. Double check the fax number.
4. Use pre-programmed numbers wherever possible.
5. Make sure your fax cover sheet states who the information is for, and mark it "Private and Confidential."
6. If appropriate, request a report sheet to confirm that transmission was OK.

This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

Guidance for sharing person identifiable information by POST



1 Confirm the name, department and address of the recipient.

2 Seal the information in a robust envelope.

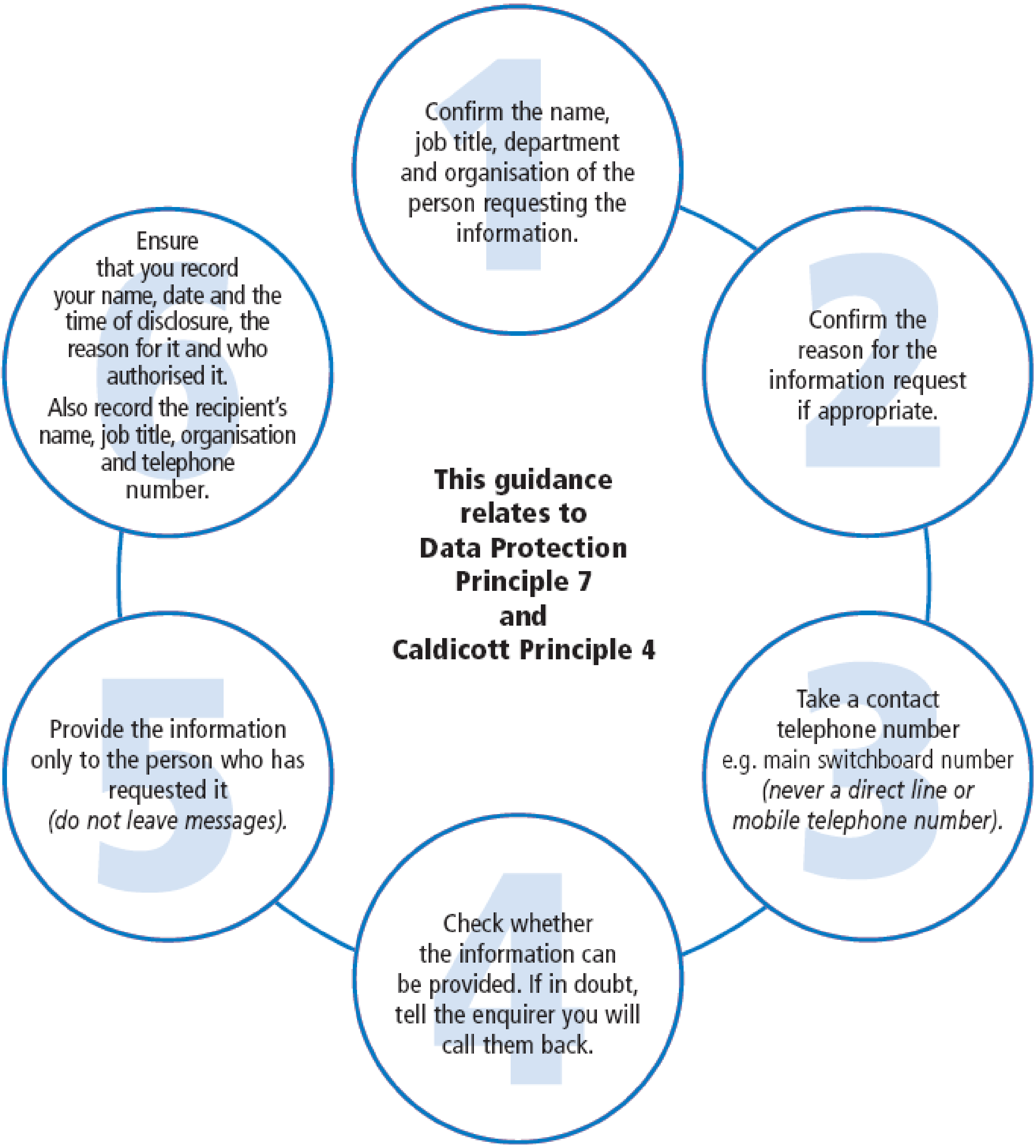
3 Mark the envelope "Private & Confidential- To be opened by Addressee Only."

4 When appropriate, send the information by Recorded Delivery.

5 When necessary, ask the recipient to confirm receipt.

This guidance relates to Data Protection Principles 6 and 7 and Caldicott Principle 4

Guidance for sharing person identifiable information by PHONE



This guidance relates to Data Protection Principle 7 and Caldicott Principle 4

1. Confirm the name, job title, department and organisation of the person requesting the information.

2. Confirm the reason for the information request if appropriate.

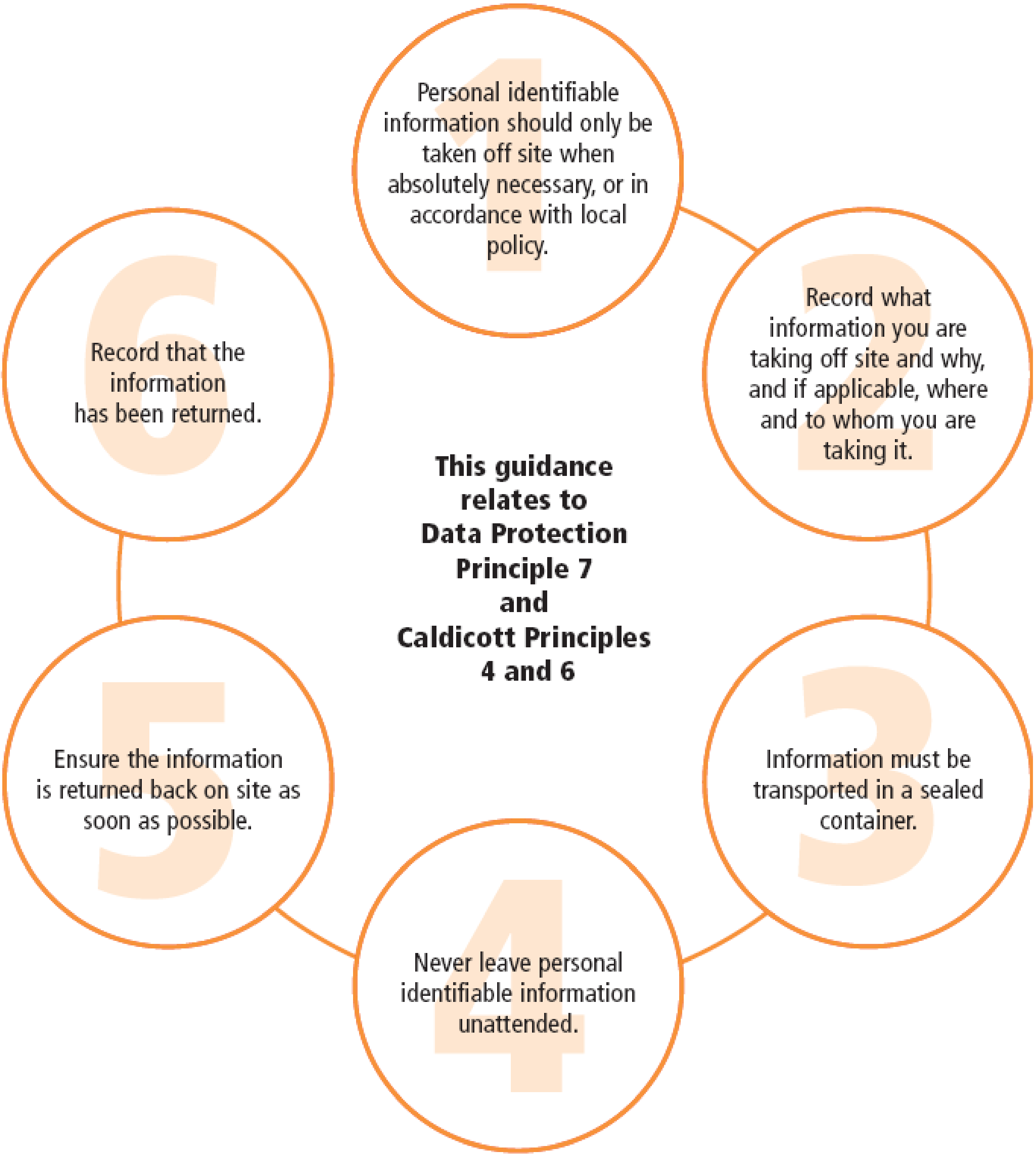
3. Take a contact telephone number e.g. main switchboard number *(never a direct line or mobile telephone number).*

4. Check whether the information can be provided. If in doubt, tell the enquirer you will call them back.

5. Provide the information only to the person who has requested it *(do not leave messages).*

6. Ensure that you record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number.

Guidance for TRANSPORTING person identifiable information



1. Personal identifiable information should only be taken off site when absolutely necessary, or in accordance with local policy.
2. Record what information you are taking off site and why, 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.
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 Principle 7 and Caldicott Principles 4 and 6

NHS
Cambridgeshire and
Peterborough
Clinical Commissioning Group

Fax

Lockton House
Clarendon Road
Cambridge
CB2 8FH

Tel: 01223 725400
Fax: 01223 725401
Safe Haven Fax: 01223 725591
Web: www.cambridgeshireandpeterboroughccg.nhs.uk

To:		Fax:	
From:		Date:	
Re:		Pages:	

□ Urgent □ For Information □ Please comment

Confidentiality Note

This communication is intended only for the use of the individual or entity to whom it is addressed and may contain information that is privileged, confidential and exempt from disclosure under law. If the reader of this communication is not the intended recipient or a representative of the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone on 01223 725400 and return it to us.

If you do not receive all the pages indicated, or if any portions of the transmission are illegible, please notify us by telephone.