Safe Haven Policy

DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Version:</th>
<th>0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ratified By:</td>
<td></td>
</tr>
<tr>
<td>Date Ratified:</td>
<td></td>
</tr>
<tr>
<td>Policy Author:</td>
<td>Essex CSU CCG IG Lead</td>
</tr>
<tr>
<td>Policy Sponsor:</td>
<td>Chief Finance Officer (SIRO)</td>
</tr>
<tr>
<td>Name of Responsible Committee:</td>
<td>Quality and Governance Committee</td>
</tr>
<tr>
<td>Date Issued:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td></td>
</tr>
<tr>
<td>Target Audience:</td>
<td>CCG Staff and Members</td>
</tr>
</tbody>
</table>

EQUALITY IMPACT ASSESSMENT

This document has been assessed for equality impact on the protected groups, as set out in the Equality Act 2010. This Policy is applicable to every member of staff within the CCG irrespective of their age, disability, sex, gender reassignment, pregnancy, maternity, race (which includes colour, nationality and ethnic or national origins), sexual orientation, religion or belief, marriage or civil partnership.
**Associated Policy Documents**

<table>
<thead>
<tr>
<th>Reference</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data Protection &amp; Confidentiality Policy</td>
</tr>
<tr>
<td></td>
<td>IM&amp;T Security Policy</td>
</tr>
<tr>
<td></td>
<td>Information Governance Policy</td>
</tr>
<tr>
<td></td>
<td>Information Lifecycle Management Policy &amp; Strategy</td>
</tr>
<tr>
<td></td>
<td>Pseudonymisation and Information Safe Havens Policy &amp; Procedure</td>
</tr>
<tr>
<td></td>
<td>Information Sharing Policy</td>
</tr>
<tr>
<td></td>
<td>Subject Access Request Procedure</td>
</tr>
</tbody>
</table>
1. CONTENTS

1. CONTENTS .................................................................................................................. 3
2. INTRODUCTION ........................................................................................................ 4
   2.1 Background ........................................................................................................... 4
   2.2 Objective ............................................................................................................ 4
   2.3 Scope .................................................................................................................... 5
   2.4 Purpose of Safe Haven ....................................................................................... 5
3. STAFF MANAGEMENT ............................................................................................... 5
4. THE PHYSICAL LOCATION OF DEVICES .............................................................. 5
5. FAX MACHINES ........................................................................................................ 6
6. PAPER DOCUMENTS ................................................................................................ 6
7. EMAILS (refer to IM&T Security Policy) ................................................................. 7
8. VERBAL COMMUNICATIONS AND TELEPHONES .............................................. 7
9. ELECTRONIC SYSTEMS ......................................................................................... 8
10. WHITE BOARDS AND NOTICE BOARDS ............................................................ 8
11. PHYSICAL SECURITY ............................................................................................. 8
12. SECONDARY USE SAFE HAVEN ........................................................................... 9
13. TRAINING ............................................................................................................. 9
14. MONITORING ...................................................................................................... 9
15. LEGAL ACTS COVERED UNDER THE POLICY ............................................... 9
16. KEY CONTACTS WITHIN THE CCG ................................................................. 9
2. INTRODUCTION

2.1 Background

The essential need to ensure that confidential patient information remains safeguarded at all times should be at the forefront of everyone working within the NHS. All persons involved in the handling of healthcare information in the NHS have a legal duty of confidence and fidelity towards the NHS bodies to which they are answerable.

All NHS Organisations already have in place procedures, which are aimed at safeguarding confidential information. Indeed, the NHS has an enviable reputation for maintaining the confidentiality of personal health data, which it acquires for the purpose of clinical care, patient administration, medical records management, wider management and planning, teaching and training, disciplinary proceedings and for the purpose of carrying out research.

It is not the intention of this guidance to disturb the existing arrangements, but rather to extend and build upon them to cover the exchange of information which the introduction of commissioning for services between NHS providers and purchasers has made more necessary.

The term “Safe Haven” was originally implemented to support contracting procedures. Today it is a term recognised throughout the NHS to describe the administrative arrangements and physical measures that must be implemented to safeguard the confidential transfer of patient identifiable information between organisations or sites using any of the following formats/methods:

Fax Machines
Post/ Email
Telephones/ Answer Phones
Computer Systems/ Electronic Media
Manual Records and Books
White Boards/ Notice Boards

2.2 Objective

To ensure that the use of patient information is handled safely, in the most secure manner, at all times, and that authorised personnel communicate information only with those who are approved and on a ‘need to know basis’. Staff who are on a ‘need to know basis’, will in some capacity, be involved in the direct delivery of a patient’s planned care.

When information is disclosed by a designated safe-haven point to an equivalent point in another organisation, (i.e. fax to fax) staff can be assured and confident that the agreed protocols will govern and protect the use of the information from that point on.
2.3 Scope

This policy applies specifically to the handling and transfer of patient confidential information; it complements the Data Protection Act 1998, the Computer Misuse Act and the NHS Caldicott Principles.

This policy does not cover the secondary use of information and “Information Safe Havens”, which is covered in the Pseudonymisation and Information Safe Havens Policy & Procedure.

2.4 Purpose of Safe Haven

The term Safe Haven describes an agreed set of administrative procedures that ensure the safe and secure handling of confidential patient information. Alternatively, the term may be referring to a designated location within an organisation, where confidential information can be sent from, received or stored in a safe and secure manner.

3. STAFF MANAGEMENT

At CCG level the Accountable Officer is ultimately responsible for security and patient confidentiality however devolved accountability for the safe transfer of patient data remains with the Caldicott Guardian.

The Executive Nurse has been appointed as the Trust Caldicott Guardian and holds responsibility for ensuring compliance with the Caldicott principles.

All staff who handle information are responsible for ensuring the information remains secure and confidential at all times. Whatever level of access is required by an individual staff member, it is important that all handling of confidential information only takes place on a strict need to know basis and only as part of his/her legitimate activity to undertake his/her job roles in the interest of providing patient care.

All staff members who are authorised to handle patient information have both a legal and professional duty to understand and comply with the law at all times.

4. THE PHYSICAL LOCATION OF DEVICES

- The physical location of “safe haven” equipment must be clearly identifiable, physically secure (i.e. a lockable room or cabinet/s) and access should ideally be via one entry point so that access can be easily controlled and monitored.

- Confidential information should only be communicated (sent or received) from a designated safe haven contact point.
5. FAX MACHINES

- Fax machines should be located in secure staff areas, which are under supervision at all times (during the opening hours of that particular facility).
- Patient identifiable information should only be sent by fax method, when it is absolutely necessary.
- The fax number should be verified with the recipient, which should already be pre-programmed into the fax.
- Newly issued numbers should always be verified and double checked prior to sending the fax.
- If there is any doubt do NOT send the document by fax transmission.
- The responsibility for the correct despatch of all fax messages is with the sender.
- Always ensure a fax cover sheet is used, clearly stating that the fax contains a confidentiality statement, and always state clearly the name of the recipient, indicating it is for their attention only, and the number of pages being sent, including the cover sheet in this count.
- It is good practice to request confirmation that the fax sent has been received safely and to obtain a copy of a report confirming the transmission was O.K.
- If the recipient’s fax is not a safe haven, telephone the recipient to let them know you are going to send a fax containing patient identifiable or confidential information.
- Gain assurances from them that they will be waiting by the fax whilst you send the information to them.
- Ask the recipient to confirm the safe receipt of the confidential information sent. Should, for any reason, they fail to notify you, it is important that you follow up immediately.
- Assurance must be obtained that they have safely received the information sent.

6. PAPER DOCUMENTS

- Patient Health Records, and all other (corporate) paper records/correspondence should always be held securely.
- In order to protect patient confidentiality you should always work with the minimum amount of person identifiable data required. Whenever possible only use Pseudonymised or de-identified data.
- A clear and tidy desk policy should be applied at all times, confidential information, under no circumstances, should be left unattended (even within secure admin areas).
- Upon completion of your administrative duties ensure that documents are returned to their designated base, updating all corresponding documentation as required.
- Sensitive information should not be worked on within public areas and under no circumstances should be left unsupervised at any time.
• Incoming mail should be opened away from public areas.
• Outgoing mail should be sealed securely and clearly marked as private and confidential; this applies to both external and internal mail.
• Traceability of Health Records is vital. If a record is being transferred to another department or to another organisation, a record should be kept at the transferred records designated base, indicating what information has been transferred by who, and to whom, detailing a date and time the transfer took place.
• Records being transferred should be transported by secure internal mail methods whenever possible. In some cases it may be necessary to arrange the transfer using a special courier service; all documentation should be securely sealed before transfer, and all necessary documentation fully completed and signed for accordingly.
• When photocopying patient identifiable information, the information should be safeguarded at all times, so that unauthorised personnel are not able to view. Always check the photocopier to ensure you have removed all corresponding paperwork before you move away from the machine, and check that there is nobody nearby who can read what you are copying.

7. EMAILS

• The CCG email system (i.e. .nhs.uk) should not be used for the transfer of patient identifiable information.
• Staff wishing to transfer identifiable information should use only the secure and approved method (NHS.Net) and only transfer to a recipient who also has a NHS.net account or approved domain such as .gcsx (the local government secure network) or .pnn (the police secure network)
• When emails are used to transfer patient identifiable information the email subject should clearly be marked “confidential”.
• Email accounts should be set up to always include a disclaimer and signature.

8. VERBAL COMMUNICATIONS AND TELEPHONES

• Requests for patient identifiable information must be fully verified to confirm the requester has a right to know before release of any sensitive information.
• Where possible the staff member should ring back the requester, (do not call unrecognised or mobile telephone numbers, use only main switchboard numbers that have been checked) which will assist in verifying the caller identity.
• If the Police request any patient identifiable information they should be directed to the CSU Information Governance Team
• All media related requests for Patient Identifiable information must always be referred to the CSU Information Governance Team
• Staff are not authorised to release any information, of any description, to the media or press.
• If you are contacting a patient directly it is important that the staff member confirms that they are talking to the correct person. Messages should not be left unless you have permission from the patient as you cannot be sure who may have access to, or hear the message. If you need to contact a patient urgently and they are not available, then you should leave your name, contact number and a very brief message asking them to return your call.

9. ELECTRONIC SYSTEMS

• Staff requiring access to clinical systems must be established as authorised.
• Access to systems will be given on a need to know basis.
• Password access is given to individuals; authorised staff should not under any circumstances allow their password to be used by others. This is a breach of the IM&T security Policy and is subject to disciplinary action.
• If using a Registration Authority Smartcard staff must ensure they comply with the terms and conditions of use as outlined by the Registration Authority Policy & Procedures
• Cards and PINs must not be left unattended either whilst logged in or out.
• Keep your password confidential, do not write it down, or leave on view for others to see.
• Passwords should be carefully chosen and not easily guessable. A mixture of alpha/numeric (letters and numbers) and special characteristics (>£$%^&!*#) is recommended.
• Ensure your password is changed regularly.
• All patient information should be stored on the network in secure folders and not on local C drives.
• Patient identifiable information must only be stored on work equipment and not in personally owned diaries, laptops or home computers.
• Only encrypted laptops, memory sticks and other removable media should be used.

10. WHITE BOARDS AND NOTICE BOARDS

• Staff must consider who may have sight of the white board/noticeboard and how this may compromise patient confidentiality. Staff are encouraged to use other, more confidential, methods of communicating when feasibly possible.

11. PHYSICAL SECURITY

• Patient identifiable information should be stored away from public areas
• Staff should adopt a clear desk policy wherever possible.
• Clinical or sensitive records should be stored in lockable cabinets
• Doors and Windows should be locked and blinds closed when unattended.
12. SECOND USE SAFE HAVENS

Please see the Pseudonymisation and Information Safe Haven Policy & Procedure for guidance on the secondary use of information.

Secondary use of information (also known as Non-healthcare medical purposes) includes the use of identifiable information for:

- preventative medicine,
- medical research,
- financial audit
- and the management of health [and social] care services

13. TRAINING

All staff should attend, as part of their induction, a session on Information Governance (which includes a section on safe haven best practice). Top-up training will be provided annually through the online Information Governance Training Tool and is mandatory for completion by all staff.

14. MONITORING

Compliance with this policy will be monitored through the use of spot checks, to assess staff understanding/compliance and visits to sites to monitor clear desks, locked screens and location of safe havens. Any incidents reported using the CCG incident reporting process will be monitored to identify breaches to this policy and such incidents will be investigated, according to their grade..

15. LEGAL ACTS COVERED UNDER POLICY

Data Protection Act 1998
Human Rights Act 1998
Access to Health Records Act 1990
Computer Misuse Act 1998
Electronic Communications Act 2000

16. RELEVANT KEY CONTACTS WITHIN THE CCG

Caldicott Guardian – Tricia D’Orsi

Senior Information Risk Owner (SIRO) – Victoria Gunn

Essex CSU IG Team – Jane Marley (jane.marley@nhs.net), Paul Cook (pcook3@nhs.net), Debbie Smith-Shaw (Debbie.smith-shaw@nhs.net), Gemma Kerr (gemma.kerr@nhs.net)
## Checklist for Approval of Policy (to be revised)

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th></th>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Title</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the title clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is it clear whether the document is a guideline, policy, protocol or standard?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><strong>Rationale</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are reasons for development of the document stated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td><strong>Development Process</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the method described in brief?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are people involved in the development identified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is there evidence of consultation with stakeholders and users?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td><strong>Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the objective of the document clear?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the target population clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are the intended outcomes described?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are the statements clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td><strong>Evidence Base</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Is the type of evidence to support the document identified explicitly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are key references cited?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are the references cited in full?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Are supporting documents referenced?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td><strong>Approval</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Does the document identify which committee/group will approve it?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Title of document being reviewed:</td>
<td>Yes/No/Unsure</td>
<td>Comments</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7. **Dissemination and Implementation**

- Is there an outline/plan to identify how this will be done?
- Does the plan include the necessary training/support to ensure compliance?

8. **Document Control**

- Does the document identify where it will be held?
- Have archiving arrangements for superseded documents been addressed?

9. **Process to Monitor Compliance and Effectiveness**

- Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?
- Is there a plan to review or audit compliance with the document?

10. **Review Date**

- Is the review date identified?
- Is the frequency of review identified? If so is it acceptable?

11. **Overall Responsibility for the Document**

- Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?

12 **Equality Impact Assessment (EIA)**

- Has an equality analysis been undertaken in preparation for this policy?
- Has the equality analysis been quality assured by the Equality and Diversity Group?

**Individual Approval**

If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

Policy ref:  
Version 0.2  
Approved:  
Review Date:  
Page 11
<table>
<thead>
<tr>
<th>Committee Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation’s database of approved documents.</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Signature</td>
</tr>
</tbody>
</table>