NHS
Herts Valleys
Clinical Commissioning Group

Checklist for the Review and Approval of Procedural Documents

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

	Yes/No/ Unsure	Comments
Title of Document		Safe Haven Policy V3
Could this policy be incorporated within an existing policy?	no	
Does this policy follow the style and format of the agreed template?	yes	
Has the front sheet been completed?	yes	
Is there an appropriate review date?	yes	
Does the contents page reflect the body of the document?	yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	yes	
Are all appendices appropriate and/or applicable?	yes	
Have all appropriate stakeholders been consulted?	yes	
Has an Equality Impact Assessment been undertaken?	yes	
Is there a clear plan for implementation?	yes	
Has the document control sheet been completed?	yes	
Are key references cited and supporting documents referenced?	yes	
Does the document identify which Committee/Group will approve it?	yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)	yes	Via staff weekly update

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.			
Name	Chief Finance Officer	Date	12/6/18
Signature	C. A.		

Committee Approval			
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.			
Name	Chief Executive Officer	Date	12/6/18
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Safe Haven Policy

Version Number	V3
Ratified By	Virtual IG Group Executive Team
Date Ratified	12 June 2018
Name of Originator/Author	Information Governance Manager
Responsible Director	Chief Finance Officer
Staff Audience	All Staff
Date Issued	July 2018
Next Review Date	June 2019

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
0.2			March 2014	
V2		Annual Review Put into new policy format.	October 2016	IG Manager
V3		Annual Review Added info about SIRO and DPO Removal of reference to @hertsvalleysccg email address.	May 2018	IG Manager

CONTENTS

Appendices:

1. INTRODUCTION

Every day the NHS collects vast amounts of information, this could be about you, your family, friends, neighbours or people that you know, but the majority of this information will belong to total strangers that you are unlikely to ever meet. This information is not the property of the NHS it belongs to the people that it has been collected from. The NHS is merely the custodian, as custodian we are responsible for the safe keeping and security of all information that comes into our keeping

As a data collector and information user you are responsible for ensuring that you handle this information with care and respect. It is your responsibility to protect this information from those who are not authorised to use it or view it. You must ensure that whilst in your care you have done everything possible to protect this information and comply with the Caldicott principles and the Data Protection Act requirements.

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/Voice recordings
Computer Systems/Electronic Media
Manual Records and Books
White Boards/Notice Boards

2. PURPOSE

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.

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

This policy does not cover the secondary use of information and “Accredited Safe Havens”.

3. DEFINITIONS

Safe Haven
The term safe haven is 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 information 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 safe haven principles.

Personal Confidential Information
Personal confidential information 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.

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 confidential information contains details of the individual’s

- Health and sexual condition
- Sexual life
- Ethnic origin
- Religious beliefs
- Trade union
- Political opinion
- Criminal convictions

4. ROLES AND RESPONSIBILITIES

The Chief Executive is ultimately responsible for security and patient confidentiality however devolved accountability for the safe transfer of patient information remains with the Senior Information Risk Owner .

4.1 Roles and Responsibilities within the Organisation

The Director of Nursing and Quality has been appointed as the CCG's Caldicott Guardian and holds responsibility for ensuring compliance with the Caldicott principles.

The Chief Finance Officer has been appointed as the CCG's Senior Information Risk Officer (SIRO). The SIRO is responsible for overall information Risk management for the organisation.

The Head of Estates and IM&T and Business Intelligence is our appointed Data Protection Officer (DPO). The DPO is responsible for ensuring that the organisation and its constituent business areas remain compliant at all times with Data Protection, Privacy and Electronic Communications Regulations..

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.

4.2 Consultation and Communication with Stakeholders

This policy will be approved by the Information Governance Group, Senior Leadership Team and by the Executive Committee

5. 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) form a designated safe haven contact point.

Fax (available via multi-functional devices)

- 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.

Fax’s must only be used when no other secure electronic method is available.

Paper Documents

- Patient Health Records, and all other (corporate) paper records/ correspondence should always be held securely.
- If personal identifiable data needs to be taken off site in paper format, security processes for this information must be followed (please refer to the information security policy)
- In order to protect patient confidentiality you must 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.
- If this information forms part of a file that is shared/provided to patients or patients representatives – a check must be made to ensure the correct information has been placed in the file.

Emails

- 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) please see
- 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.

Verbal Communication 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 call 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 CCG Information Governance Team
- All media related requests for Patient Identifiable information must always be referred to the CCG 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.

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.
- Staff must lock their screens when away from their desks.
- 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.

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.

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.

6. MONITORING COMPLIANCE

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.

.

7. EDUCATION AND TRAINING

All staff attend, as part of their induction, a session on Information Governance. Top-up training will be provided annually through the online Information Governance Training Tool and is mandatory for completion by all staff.

8. REFERENCES

GDPR/Data Protection Act (DPA) 2018
Freedom of Information Act 2000
Controlled Environment for Finance (CEfF)

9. ASSOCIATED DOCUMENTATION

Information Security Policy
Information Risk Policy
Email & Intranet Policy
IG A Guide for Staff

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.
Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	HVCCG Safe Haven Policy
What is it that is being proposed?	This policy sets out the CCG’s commitment to preserve the confidentiality, integrity and availability of information and information systems and to ensure the information and systems are effectively and lawfully managed.
What are the intended outcome(s) of the proposal	That all CCG staff are aware of their responsibilities and are aware of legal requirements and CCG processes.
Explain why you think a full Equality Impact Assessment is not needed	This policy sets out the information governance requirements in relation to information security requirements.
On what evidence/information have you based your decision?	The policy refers to the security of the information asset and to the system that the information may be stored on.
How will you monitor the impact of policy or service?	Via the IG Data Protection and Security Toolkit
How will you report your findings?	To the Senior Leadership Team via the IG Data Protection and Security toolkit action plans and compliance reports
Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a	

full Equality Impact Assessment is not required.	
Assessors Name and Job title	Ruth Boughton
Date May 2018	Information Governance Manager