NHS
West Essex
Clinical Commissioning Group

Safe Haven Policy

Policy Reference: IG03

Brief Summary:
This policy sets out the safe haven principles the Clinical Commissioning Group and all of its staff members must implement into their daily working practices. This is to ensure the protection of confidentiality of patient information at all times, during transferor communication with NHS trusts or other authorised partners

Compliance with all CCG policies, procedures, protocols, guidelines, guidance and standards is a condition of employment. Breach of policy may result in disciplinary action.

Document Management

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	14/03/2013	Draft	New Document	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.0	03/12/2014	Draft	Amendments made following comments from IG Steering Group	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.1	18/12/2014	Draft	Key Contacts Added following amendments	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
1.2	05/03/2015	Final	Approved by West East CCG Board	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)
3.0	07/10/2016	Final	Review approved by West East CCG Executive Committee	CCGs Information Governance Team (Hosted by Basildon and Brentwood CCG)

For more information on the status of this policy, please contact:	
NHS West Essex Essex CCG	Information Governance Team
Approved by	Executive Committee
Approval Date	7th October 2016
Next Review Date	March 2019
Responsibility for Review	CCG's Information Governance Team
Audience	All NHS West Essex CCG officers and staff (which includes temporary staff, contractors and seconded staff).

Contents

1. Introduction

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

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 purposes of clinical care, patient administration, medical records management, wider management and planning, teaching and training, disciplinary proceedings and for 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 or methods:

Fax Machines

Post / E-mail

Telephones / Answer Phones

Computer Systems / Electronic Media

Manual Records and Books

White Boards / Notice Boards

2. Purpose

The purpose of this policy is to ensure that the use of patient information is handled safely, in the most secure manner at all times and that authorised personnel communicate 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, (that is 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.

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 (1990) and the NHS Caldicott Principles.

4. Definitions and terms

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.

5. Roles and Responsibilities

Accountable Officers for NHS West Essex CCG

The Chief Officer (CO), as the Accountable Officer, has overall responsibility for information governance within the CCG. The is responsible for the management of Information Governance and for ensuring appropriate CO mechanisms are in place to support service delivery and continuity.

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.

Senior Information Risk Owner (SIRO) for NHS West Essex CCG

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Director of Finance, Contracting and Performance. The SIRO takes ownership of the organisation's

information risks policy and acts as advocate for information risk on the CCG Governing Body and Audit Committee. This includes oversight of information security incident reporting and response arrangements.

Caldicott Guardian for NHS West Essex CCG

The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patients / service users information and enabling appropriate sharing. For the CCG this is an executive Chief Medical Officer. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to do so and will advise on options for lawful and ethical processing of information.

All Staff

The majority of staff handle information in one form or another. Staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to relevant legislation, case law and national guidance.

All staff who handle information are responsible for ensuring this 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.

The CCG policies and procedures will reflect such guidance and compliance with these strategies and will ensure a high standard of Information Governance compliance within the organisation. All staff and officers whether permanent, temporary, contracted, agency or contractors are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

6. Physical Location of Devices

The physical location of “safe haven” equipment must be clearly identifiable, physically secure (that is a lockable room or cabinets) and access should ideally be via one entry point only so that this can be easily controlled and monitored.

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

7. 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, this 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 dispatch of all fax messages is with the sender.
- Always ensure a fax cover sheet is used clearly stating that it contains a confidentiality statement and always clearly state the name of the recipient, indicating it is for their attention only and the number of pages being sent, include the cover sheet in this count.
- It is good practice to request confirmation that the sent fax has been received safely and to obtain a copy of a report confirming the transmission was successful.
- If the recipient's fax is not a safe haven, telephone 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.
- Ask the recipient to confirm the safe receipt of the confidential information sent. Should they fail to notify you for any reason, it is important that you follow this up immediately.
- Assurance must be obtained that they have safely received the information sent.

8. 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 anonymised 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 administrative 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, documentation 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, this 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.

9. E-mails

- Staff wishing to transfer identifiable information should use only the secure and approved method (NHS.net) and only transmit 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 e-mails are used to transfer patient identifiable information the subject should be clearly marked “confidential”.
- E-mail accounts should be set up to always include a disclaimer and signature.

10. 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 Information Governance Team.
- All media related requests for patient identifiable information must always be referred to the 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.

11. 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 Acceptable Use of IT 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 NHS North East London Commissioning Support Unit 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.

12. 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 feasible.

13. 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.

14. Secondary Uses

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

15. Audit and Monitoring Compliance

The CCG will use a variety of methods to monitor compliance with the processes in this policy, including as a minimum the following two methods:

IG Incidents
Information Governance compliance will be monitored quarterly through the review of reported IG incidents by the IG Steering Group.

The IG Steering Group has a responsibility to provide assurances that this framework is adequate to offering clear guidance in the event of significant changes which may affect the framework. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programs and progress reports

- Reporting Information Governance Toolkit (IGT) assessments and improvement plans
- Communicating IG developments

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework as a response to the identification of any gaps, or as a result of the detection of risks arising from this prompted by incident review, external assessments or other sources of information and advice.

16. Dissemination and Implementation

The policy will be published on the intranet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content or change in process will be through electronic channels for example through e-mail, in bulletins and so on.

Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the SIRO.

17. Training

All staff likely to be in post 3 months or longer (permanent, temporary, contracted or seconded) are required to complete the online mandatory IG training modules (https://www.igtt.hscic.gov.uk/igte/index.cfm) within one month of joining, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles. A Training Needs Analysis (TNA) has been developed for staff in key roles, as part of effective delivery of training program.

However, should staff have access to personal identifiable information, training should be completed within 1 week, regardless of intended service length.

18. Related documents

The following documentation relates to the management of information and together underpins the CCG's Information Governance Assurance Framework. This policy should be read in conjunction with other policies:

- Information Governance Policy
- Data Protection Act & Confidentiality Policy
- Information Sharing Policy
- Acceptable Use of IT Policy

- Information Lifecycle Management Policy & Strategy
- Acceptable Use of Electronic Communications Policy
- Access to Information Policy

Legal Acts Covered under this Policy:

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

19. Equality and Diversity

The CCG recognises the diversity of the local community and those in its employment. The CCG aims to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. 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.

20. Key Contacts within the CCG

Senior Information Risk Owner	Director of Finance, Contracting and Performance
Caldicott Guardian	Chief Medical Officer
CCG IG Champion	Governance and Risk Manager

Information Governance Team

Jane Marley	Head of Information Governance	jane.marley@nhs.net
Tracey van Wyk	IG Lead	tracey.vanwyk@nhs.net
Ian Gear	FOI Lead	iain.gear@nhs.net
Debbie Smith-Shaw	Information Governance Adviser	debbie.smith-shaw@nhs.net