NHS
North East Hampshire and Farnham
Clinical Commissioning Group

SAFE HAVEN POLICY

Document information

Document type:	Operational Policy
Document reference:	
Document title:	**Safe Haven Policy**
Document date:	April 2013
Author:	NHS South Commissioning Support Unit, Information Governance Team North East Hampshire & Farnham Clinical Commissioning Group
Approved by:	Audit & Risk Committee
Approval date:	30 September 2015
Ratified by Corporate Governance review Group:	
Version:	V1.2
Review date:	September 2017

SAFE HAVEN POLICY

Contents

1. Summary

This Policy is written to give NHS North East Hampshire & Farnham Clinical Commissioning Group (CCG) staff a clear Safe Haven framework which includes advice and guidance and to inform staff of their operational and legal responsibilities.

2. Consultation

The Policy has been considered by the CCG Corporate Governance Review Group which includes the CCG Caldicott Guardian and the Senior Information Risk Officer. Comments have been incorporated as appropriate.

3. Introduction

In order to comply with legislation and DH guidance, all NHS organisations are required to have safe haven procedures to safeguard the privacy and confidentiality of personal or sensitive information held.

4. Scope and Definitions

The aim of this policy is to ensure that CCG operates such procedures ensuring that confidential or sensitive information sent to or from the CCG is handled in such a way as to minimise the risk of inappropriate access or disclosure.

5. Safe Haven

A 'Safe Haven' is a term used to explain either a secure physical location or the agreed set of administration arrangements that are in place within the Trust to ensure confidential patient or staff information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the Trust 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.

Personal information is information which can identify a person – in which the person is the focus of the information and links that individual to details which would be regarded as private e.g. name and private address, name and home telephone number etc.

6. Sensitive Personal Information

Sensitive personal information is where the personal information contains details of that person's:

- Health or physical condition;
- Sexual life;
- Ethnic origin;
- Religious beliefs;
- Political views;
- Criminal convictions.

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

7. Where Safe Haven Procedures should be in Place

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

8. Sending Confidential Information

- Always consider whether it is necessary to release personal information
- Send personal - identifiable data only when it is essential to do so
- Within the NHS, confidential information should always be addressed to the safe haven of the recipient's organisation and marked confidential.

9. Processes/Requirements

9.1 Post

- All incoming mail should be opened away from public areas. Outgoing mail (both internal and external) should be sealed securely and marked 'private and confidential' if it contains person-identifiable information.
- Where possible send post to a named person.
- Staff sending documents by external post or courier, use a 'signed for' delivery service. Use appropriate stationery, such as reinforced envelopes or document wallets when necessary. Check that the address is typed or written clearly in indelible ink.
- When staff are sending mail outside of the NHS, send documents only to known, named, authorised personnel marked 'Confidential'.
- Use as risk assessment and register if appropriate

9.2 Paper Documents

- All sensitive records must be stored face down in public areas and not left unsupervised at any time.

- Information that is no longer required (e.g. post it notes, messages) should be shredded or disposed of under confidential conditions

- Make a log of what notes have left the department (e.g. home visits etc).

- Ensure that documents are properly 'booked out' of any relevant filing system if necessary, and records kept of what is sent and where. Copies should be sent or retained, as appropriate

9.3 Computers

- Do not share logons and passwords with anyone

- 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 personal data.

- PCs or laptops should be locked or switched off when you are away from your desk for any length of time.

- Information should be held on the organisation's network servers, not stored on local hard drives or removable media.

- Information must not be saved or copied into any PC or media that is 'outside the NHS'.

- All person-identifiable information sent by email **must** be sent from one NHS Mail address to another secure e-mail domain such as NHS.net to NHS.net or via an encrypted attachment

9.4 Telephone Calls

- Do not make telephone calls where you can be overheard (e.g. Reception)

- When you receive a call, check to ensure you are speaking to the correct person, ring back (where possible) to confirm someone's identity.

9.5 Physical Location and Security

- Do not allow unauthorised people into areas where confidential information is kept unless supervised. Check peoples ID badges.

- Take measures to prevent casual scanning of information.

- Store person-identifiable information in a locked drawer/filing cabinet.

9.6 Legal Compliance

This policy ensures compliance with:

- Data Protection Act 1998;
- Common Law of Confidentiality;
- Confidentiality: NHS Code of Practice;
- Caldicott Principles.

10. Sharing information with other organisations (Non NHS)

Staff sharing personal information with other agencies should be aware of the Pan Hampshire Inter-agency Information Sharing Protocol and the requirement to have an Information Sharing Agreement in place for the routine sharing of person identifiable information. This will provide the CCG with the assurance that these organisations are able to comply with the safe haven ethos and meet legislative and related guidance requirements.

11. Responsibilities

The CCG has a particular responsibility for ensuring that it meets its corporate and legal responsibilities, and for the adoption of internal and external governance requirements. The CCG *Senior Management Team* is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

11.1 CCG Accountable Officer

The CCG Accountable Officer has overall responsibility for governance in the CCG. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity

11.2 Caldicott Guardian

The CCG Caldicott Guardian has a responsibility for reflecting patients' interests regarding the use of personal identifiable information. They are responsible for ensuring all personal identifiable data is shared in an appropriate and secure manner.

11.3 Senior Information Risk Officer

The CCG Senior Information Risk Officer (SIRO) is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy. For ensuring the Corporate Risk Management process includes all aspects of Information risk. And for ensuring the CCG *Audit & Risk committee* is adequately briefed on information risk issues.

11.4 Head of Information Governance

The Head of Information Governance is responsible for ensuring that this Safe Haven policy is implemented and that Information Governance systems and processes are developed and training is available and is also responsible for the overall development and maintenance of information management practices.

11.5 Data Custodians

To raise the profile of Information Governance throughout the CCG and to provide local 'champions', the CCG has established a network of Data Custodians. These individuals are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets and for ensuring all staff must complete the appropriate modules of the Information Governance Training Toolkit. This role is in addition to their duties and should be fully supported by their manager and recognised in their job description.

Data Custodians will also, on an annual basis, be responsible for local assessment of data collections to establish an Information Assets Register (IAR) and also audit staff

compliance with Information handling requirements. This important task provides a Cluster wide inventory to inform the annual registration with the Information Commissioner and highlights potential risk areas that may need risk management intervention. Information Assets (IAs) should include any operating systems, infrastructure, and business applications, off the shelf products, services, user-developed applications, records and information held.

Support in the role is available at any time from the CSU Information Governance Team. The CCG values staff comments regarding Information handling arrangements and training and it is hoped that each Data Custodian will act as a further conduit to voice these comments.

11.6 CCG Audit & Risk Committee
It is the role of the CCG Audit & Risk Committee to define the CCG policy in respect of Information Governance, taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

11.7 CCG Service Leads
Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance.

11.8 CCG Staff
All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

11.9 Training
All new staff will be made aware of the existence of this policy via the induction process and a copy will be available on the intranet. Managers must highlight to staff their responsibility to ensure that they are aware of the content of this policy and remind staff of the “non-disclosure of confidential information clause” in their staff contract.

12. Success Criteria

Reference Documentation

Copyright, Designs & Patents Act 1988

Computer Misuse Act 1990

Caldicott Report 1997

The Data Protection Act 1998

The Data Protection Act 1998 (Employers Code of Practice)

The Human Rights Act 1998

Electronic Communications Act 2000

Regulation of Investigatory Powers Act 2000

NHS Confidentiality Code of Practice 2003

Records Management NHS Code of Practice 2006

NHS Information Security Management Code of Practice 2007

13. Equality, diversity and mental capacity

This policy was assessed against the CCG Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time.

This policy has been assessed and meets the requirements of the Mental Capacity Act 2005

14. Consultation and trials

This policy review has taken into account comments received from the CCG Corporate Governance Review Group and has been viewed by the Senior Information Risk Officer, Caldicott Guardian,

15. Communication and dissemination

This policy will be communicated and disseminated by means of the CCG Intranet. Additional/alternative dissemination arrangements will be included as they become available.

16. Policy Review

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are to be introduced).