NHS
Surrey Downs
Clinical Commissioning Group

Safe Haven Policy

Policy ID	IG05
Version:	1.1
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Executive Committee
Date agreed	2nd November 2015
Next review date:	2nd November 2017

Improving care together across Surrey Downs

Summary

The aim of this policy is to ensure that Personal Confidential Data (PCD) or commercially sensitive information sent to or from the Surrey Downs Clinical Commissioning Group is handled in such a way as to minimise the risk of inappropriate access or disclosure.

Version History

Version	Review Date	Name of Reviewer	Ratification Process	Notes
0.1	27/10/2013	NHS South CSU IG Team	Draft	New document
1.0	29/09/13	NHS South CSU IG Team	Final	Approved by Governing Body
1.1	02/11/2014	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect to recent Health and Social Care (Safety & Quality) Act 2015 and Caldicott 2 Review.
Contributors		Governing Body Secretary, Head of Planning & Performance and, South East CSU Information Governance Principle Associate.		
Audience		All CCG officers, Governing Body members and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.		

Equality Statement

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality Analysis

This policy has been subject to an Equality Analysis, the outcome of which is recorded below.

1. Does the document/guidance affect one group less or more favourably than another on the basis of:			
	• Race	Yes, No or N/A	Comments
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the document/guidance likely to be negative?	N/A	
5	If so, can the impact be avoided?	N/A	
6	What alternative is there to achieving the document/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

Contents

Safe Haven Policy

1. Introduction

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

2. Scope

The aim of this policy is to ensure that Personal Confidential Data (PCD) or commercially sensitive information sent to or from the Surrey Downs Clinical Commissioning Group (the CCG) is handled in such a way as to minimise the risk of inappropriate access or disclosure.

3. Safe Haven Definition

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 CCG to ensure confidential service user information, staff or business information is communicated safely and securely. It is a safeguard for confidential information, which enters or leaves the CCG whether this is by fax, email, post or other means. Any members of staff handling confidential information, whether paper based or electronic must adhere to the Safe Haven principles.

3.1 Personal Confidential Data (PCD)

Personal Confidential Data (PCD) is sufficient personal information about identified/identifiable individuals, which should be kept private/secret and includes dead as well as living people. This includes a combination of:

- Name, address, postcode, Date of Birth & NHS number;
- the racial or ethnic origin of a data subject;
- their political opinions & their sexual life;
- their religious beliefs or other beliefs of a similar nature;
- the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed;
- whether a member of a trade union.

3.2 Corporate-Confidential Data

Any information which is defined **as such** by the CCG is essential to the core function of the organisation, not already in the public eye and, if available in the wrong hands may cause reputational damage. Examples include:

- Operational budgets;
- quotes, tenders and contracts,
- Legal advice and investigations, (Not normally for general release under the Freedom of Information Act (2000) unless an exemption applies).

3.3 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.

4. Processes/Requirements

4.1 Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules must apply:

- Ensure it is sited in an area that is restricted to those who need to access the information.
- 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.
- Notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- The confirmation of receipt should be checked to ensure the fax has been transmitted to the intended recipient, where possible the receipt should be attached to the original document.
- Where possible the NHS number should be used for identification in preference to the patient's name and address.
- Care is taken in dialing the correct number.
- Confidential faxes are not left lying around for unauthorised staff to see.
- Only the minimum amount of personal information should be sent.
- All confidential faxes sent should be clearly marked 'Private and Confidential' on the front sheet.
- Frequently used numbers should be programmed into the fax machine 'memory dial' facility. This will minimise the risk of dialing incorrect numbers.

- In clinical areas the Safe Haven should be in a room/area where any incoming fax, letters or emails can be received in privacy and retrieved only by authorised personnel.
- If you receive a call requesting that confidential information be sent via fax always call the requestor back to confirm the caller's identity using an independent number source.
- Always seek advice from your line manager or the Information Governance team if you are unsure whether or not to send any information via fax.
- If it is highly sensitive ensure someone is at the receiving end waiting for it.
- Ensure only authorised staff handle confidential information.
- If you receive faxes that contain personal information store them in a secure environment.
- Fax machines should be turned off out of hours.

4.2 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 a risk assessment and register if appropriate

4.3 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

4.4 Computers

- Do not share log-ons 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 of a sensitive or confidential nature 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 NHSmail address to another secure email domain such as NHS.net to NHS.net or via an encrypted attachment.

4.5 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.

4.6 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 hard copies of PCDs and commercially sensitive information in a locked drawer/filing cabinet.

5. Sharing Information

Since the introduction of the Health and Social Care (Safety & Quality) Act 2015, on 1 October 2015, Health and Social Care bodies have two new duties: to share relevant information for the direct care of an individual and to include the NHS Number when doing so.

The 2013 Caldicott Review 'Information: to Share or not to Share' identified that a 'culture of anxiety' prevented the appropriate sharing of people's information in support of direct care. The new duty requires health and adult social care bodies to share information that is relevant to the direct provision of a person's care with other organisations directly involved in their care and treatment.

The default position should be to share unless there is a reason not to.

The new duty to use the NHS number does not require those without access to the NHS Number to use it, nor for them to do so where this would require unreasonable

effort, but, reflecting current best practice, where the requirement can be met is it now a legal requirement to do so.

When sending PCD or commercially sensitive information:

- Always consider whether it is necessary to release personal information
- Send PCD 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.

Staff sharing PCD with other agencies should be aware of the Health and Social Care Information Sharing Framework and the requirement to have an Information Sharing Agreement in place for the routine sharing of PCD. 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.

6. Roles and Responsibilities

6.1 Accountable Officer

The CCG's Accountable Officer has overall responsibilities for the management of information governance and ensuring appropriate mechanisms are in place to support service delivery and continuity in their organisations. The Accountable Officer has delegated operational information governance responsibilities to the CCG's Senior Information Risk Owner (SIRO).

6.2 Senior Information Risk Owner

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Chief Finance Officer (CFO). The SIRO takes ownership of the organisation's information risks and act as advocate for information risk to the CCG Governing Body, Executive Committee and Audit Committee by providing written advice on the organisation's information security incident reporting and response arrangements.

6.3 Caldicott Guardian

Caldicott Guardians in the NHS ensure a harmonised approach to information management and the protection of patient/service-users' confidentiality. The CCG's Caldicott Guardian is a member of the Governing Body from clinical background.

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for managing patient data, particularly PCD. Acting as the 'conscience' of the CCG, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

6.4 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff (Directors and Heads of Departments) responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

Ownership of assets is related to the position held and remit, rather than an individual. Any handover of responsibilities should be accompanied by a formal handover of information assets, all relevant information, processes and procedures.

6.5 Data Custodians

Information Asset Owners can appoint Data Custodians to support in the delivery of their information risk management responsibilities. Data Custodians ensure that policies and procedures are followed, recognise actual or potential security incidents and **take** steps to mitigate those risks, consult with their IAOs on incident management and ensure that information asset registers are accurate and up to date.

Data Custodians for the organisation have been identified as existing post-holders of varying levels of seniority, dependent on the business need of the team.

6.6 All Staff

The majority of staff handle information in one form or another. Staff who 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.

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

7. Training Mandatory IG Training for all staff

The CCG recognise the importance of an effective training structure and programme to deliver compliant awareness of IG and its integration into the day-to-day work and procedures.

All permanent/temporary/contract staff including lay members will complete the online mandatory training modules within first week of employment, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles.

9. Reference Documentation

- Health and Social Care (Safety & Quality) Act 2015
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Caldicott Report 1997 and 2013
- The Data Protection Act 1998
- The Human Rights Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Copyright, Designs & Patents Act 1988

10. Dissemination and Implementation

The policy will be publicised on the internet. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content/change in process will be through email/staff bulletin in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the Chief of Corporate Affairs - SIRO.

11. Related CCG documents

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

- Information Governance Policy
- Confidentiality Policy - Data Protection
- Records Management Policy
- Subject Access Request Policy
- Information Security Policy
- IG and Cyber Security Incident Management and Reporting Procedure