NHS
Surrey Downs
Clinical Commissioning Group

Confidentiality Policy – Data Protection Act 1998

Policy ID	IG07
Version	3.0
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Executive Committee
Date agreed	27th October 2015
Next review date:	20th October 2017

Improving care together across Surrey Downs

Summary

This Policy has been written to guide all Surrey Downs Clinical Commissioning Group staff so that they are aware of their legal duty to maintain confidentiality. It outlines guidance and standards that MUST be followed by all staff in order to protect personal and corporate confidential information.

Version History

Version	Review Date	Name of Reviewer	Ratification Process	Notes
1.1	27/01/2015	NHS South CSU IG Team	Final	Approved by Executive Committee
1.2	09/07/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect Policy to reflect recent IG Toolkit guidelines, IG accountability and responsibility, dissemination and implementation process in the organisation. Confidentiality Agreement for Third Suppliers has been removed from document.
2.0	21/07/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	Approved by Executive Committee
2.1	24/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect to reflect new CCG SIRO
3.0	27/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	SIRO changes approved by Executive Committee
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

Confidentiality Policy

1. Introduction

NHS Surrey Downs Clinical Commissioning Group (the CCG) has a legal obligation to comply with all appropriate legislation in respect of, Confidentiality and Data Protection, Information Security Records Management. It also has a duty to comply with guidance issued by NHS England, the Information Commissioner, other advisory groups to the NHS and guidance issued by professional bodies.

2. Definitions

This Confidentiality Policy details how the CCG will meet its legal obligations and NHS requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Data Protection Act 1998 as that is the key piece of legislation covering security and confidentiality of personal information.

3. Legislation

For the purpose of this Policy other relevant legislation and appropriate guidance may be referenced. The legislations listed below also refer to issues of security of personal confidential data:

- Data Protection Act 1998
- Access to Health Records 1990
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Health and Social Care Act 2012

4. NHS & Related Guidance

The following are the main publications referring to security and or confidentiality of personal confidential data:

- Confidentiality: NHS Code of Practice
- Records Management: NHS Code of Practice
- Information Security: NHS Code of Practice
- Employee Code of Practice (Information Commissioner)
- Caldicott Report 1997 and 2013

5. Roles and Responsibilities

5.1 Accountable Officer

The Accountable Officer in the CCG has overall responsibilities for the management of information governance and ensuring appropriate mechanisms are in place to support service delivery and continuity in the organisation.

The implementation of, and compliance with this Policy is delegated to the CCG's Governing Body Secretary who will have responsibility for bringing Information Governance (IG) issues to the attention of the CCG Executive Management Team. The Governing Body Secretary will work closely with the designated Information Governance Manager from South East Commissioning Support Unit (SE CSU) to ensure that all tasks delegated to SE CSU meets the required standards in line with the existing contract/s or Service Level Agreement/s (SLAs).

Key SE CSU tasks include:

- Maintaining registrations
- Facilitating training sessions
- Advising on subject access requests
- Acting as initial point of contact for any IG issues which may arise within the CCG
- Providing reports to the CCG Information Governance Steering Group (IGSG) and the Executive Management Team as required
- Auditing data protection compliance
- Facilitating action in areas identified as being non-compliant
- Assisting with complaints concerning data protection breaches

5.2 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.

5.3 Caldicott Guardian

The CCG's Caldicott Guardian is a member of the Governing Body and the Information Governance Steering Group (IGSG) from clinical background. 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. The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for managing patient data, particularly Personal Confidential Data (PCD).

5.4 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are senior managers 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.

5.6 Data Custodians

IAOs have Data Custodians to support in the delivery of their information risk management responsibilities within their directorate/team. 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 a list of information assets are accurate and up to date.

5.7 All Staff

All staff have a legal duty of confidence to keep PCD and commercially sensitive data secure and private, and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and should ensure that:

- Confidential information is not discussed in public places or where they can be overheard.
- PCDs or commercially sensitive information are not lying around unattended, this includes telephone messages, computer printouts, faxes and other documents or, leave a computer logged on to a system where personal confidential data can be accessed.
- Access to confidential information must be on a need-to-know basis.
- Disclosure of PCDs or commercially sensitive information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure must be discussed with either their Line Managers or the CCG's Governing Body Secretary or the IG Manager.

Access to rooms and offices where PCDs or commercially sensitive information are stored must be locked and controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of confidential information by unauthorised parties.

All staff should clear their desks at the end of each day. In particular they must keep all records containing confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing PCDs or commercially sensitive information must be put into a confidential waste bin. Printouts and fax messages must not be left lying around but be filed and locked away when not in use.

6. Security & Confidentiality

All confidential information relating to identifiable individuals and any information that may be deemed commercially sensitive must be kept secure at all times. The CCG will ensure there are adequate policies and procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information.

7. Database Management

The CCG will ensure that all databases that require registration are registered in accordance with the Act's requirements and these registrations are reviewed on a regular basis. Each computer system/database will have a designated contact/administrator. A list of these nominated personnel will be maintained by the CCGs.

For the purposes of this Policy the term "Database" refers to a structured collection of records or data held electronically which contains personal confidential data. In the event that further guidance is needed in respect to what constitutes a database please contact the SE CSU ICT Team.

8. Disclosure of Information & Information in Transit

It is important that information about identifiable individuals (such as the general public and/or staff) should only be disclosed on a strict need to know basis. Strict controls governing the disclosure of identifiable information is also a requirement of the Caldicott recommendations.

All disclosures of computer held identifiable information should be included in the relevant Information Asset Register.

Some disclosures of information may occur because there is a statutory requirement upon the CCGs to disclose e.g. with a Court Order or because other legislation requires disclosure (for staff to the tax office, pension agency)

If personal confidential information needs to be transported in any media such as: disc, memory stick or manual paper records, this should be carried out to maintain strict security and confidentiality of this information.

Contracts between the CCGs and third parties must include an appropriate confidentiality clause that must be disseminated to the third parties employees.

9. Disclosure of information outside the European Economic Area (EEA)

No personal data should be disclosed or transferred outside of the EEA to a country or territory which does not ensure an adequate level of protection unless certain exemptions apply or adequate protective measures are taken.

In the event that there is a need to process confidential information outside of the United Kingdom, the Governing Body Manager or the designated IG Manager must be consulted prior to any agreement to transfer or process the information.

10. Disclosing Personal Confidential Data

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager or the Governance Body Secretary or designated IG Manager before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient/service user's information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss the Governance Body Secretary or designated IG Manager before disclosing, who will inform and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or the Governance Body Secretary or designated IG Manager or before disclosing, who will inform and obtain approval of the Caldicott Guardian.

When necessary a Data Sharing, Data Re-Use or Data Transfer Agreement should have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the CSU IG Team.

Care must be taken when transferring information to ensure that the method used is secure. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, emails, faxes and post. See the Safe Haven Procedure for guidance on the safe transfer of person confidential data.

CCG Staff may only transfer personal, confidential or commercially sensitive information by using either an NHS.net account or Secure File Transfer. Staff should also be aware that this security is only assured if the email is transferred by nhs.net to one of the following other secure email addresses:

another NHS.net account	x.gsi.gov.uk	gsi.gov.uk
gse.gov.uk	gsx.gov.uk	pnn.police.uk
cjsm.net	scn.gov.uk	gcsx.gov.uk
mod.uk		

If information is required to be sent to a member of the public, using their non-secure email address, it is the responsibility of the member of staff to ensure that the member of public is provided with a clear explanation of the risks of using unsecure email addresses and consent should be obtained.

There are Acts of Parliament that govern the disclosure of personal information. Some of these Acts make it a legal requirement to disclose and others that state that information cannot be disclosed. These Acts are detailed below:

- Public Health (Control of Diseases) Act 1984
- Public Health (Infectious Diseases) Regulations 1985 & 1998
- Education Act 1944 (for immunisations and vaccinations to NHS Public Health England from schools)

- Births and Deaths Act 1984
- Police and Criminal Evidence Act 1984
- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- Children Act 2004

In the event that a request for disclosure is made referencing any of these Acts the Governing Body Secretary and the IG Manager be notified prior to any information being released.

11. Working away from the office environment

There will be times when staff may need to work from another location or while travelling. This means that these staff may need to carry the CCG's information with them which could be confidential in nature e.g. on a laptop, USB stick or as paper documents.

Taking home/removing paper documents that contain personal confidential data from CCG's premises should be discussed with your line manager to identify potential risks.

When working off site, staff must ensure that their working practice complies with the CCG's Mobile Working Policies. Any removable media must be encrypted to the current NHS Encryption Guidance/Standards.

Staff must not leave confidential information unattended whilst travelling and ensure that it is kept in a secure place if they take it home or to another location.

Staff must minimise the amount of person confidential data that is taken away from CCGs' premises.

If staff need to carry personal confidential data they must ensure that any personal information is transported in an appropriate and secure manner and is kept out of sight whilst being transported.

Staff are responsible for ensuring that any information taken home is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must not forward any personal confidential data via email to their home email account. Staff must not use or store personal identifiable or confidential information on a privately owned computer or device.

12. Training

All new starters to the must undertake Information Governance training via the online IG Training Tool, to include compliance with the Data Protection Act and general IT security training, as part of the induction process. Extra training in these areas will be given to those who need it such as Data Custodians and those dealing with requests for information. A register will be maintained of all staff who have completed the online training and those who have attended face to face induction sessions.

Annual IG refresher training should be undertaken by all CCGs staff via the Information Governance Training Tool.

All staff will be made aware of what could be classed as an information security incident or breach of confidentiality. They will be made aware of the process to follow and the forms to complete, so that incidents can be identified, reported, monitored and investigated. Please see the CCGs Information Governance SIRI Reporting Policy for further guidance on this area.

13. Contracts of Employment

All contracts of employment include a clause on data protection and general confidentiality. All temporary/contractors/agency staff (third party staff) with access to the CCG systems, premises, data/information must be sign the CCG's Confidentiality Agreement for Third Staff.

14. Abuse of Privileges, and Disciplinary

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. All staff should be aware breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

15. Confidentiality Audits

Good practice requires that all organisations that handle personal confidential data put in place processes to highlight actual or potential confidentiality breaches in their

systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the CCG Data Custodian through a programme of audits.

Members of staff who would like access to their personal confidential information must submit a subject access request under the Data Protection Act 1998 to the Governing Body Secretary. Please refer to the CCGs' Subject Access Request Policy for guidance on how to request or handle a Subject Access Request.

16. Dissemination and Implementation

The Policy will be publicised on the website. 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 the 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 Governing Body Secretary or the IG Manager.

17. Related Documents

The following documentation relates to the management of information and together underpins both CCG's Information Governance Assurance Framework. The Information Governance Framework should be read in conjunction other documents, including, but not limited to:

- Information Governance Policy
- Information Security Policy
- Remote Working Portable Devices Policy
- Safe Haven Policy
- Subject Access Request Policy
- Data Protection and Confidentiality Policy
- Records Management Policy
- Freedom of Information Policy
- Registration Authority Guidance
- Information Incident Management and Reporting Procedures
- Confidentiality Agreement for Third Party Staff/Contractors

18. Monitoring & Audit

This Policy will be monitored by the CCG's Information Governance Steering Group (IGSG) to ensure any legislative changes that occur before the review date are incorporated. The Policy will also be reviewed biennially or when changes to legislation necessitate an earlier review.

Appendix 1: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to your line Manager, Governing Body Secretary and the Information Governance Manager. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns their Line Manager or the IG Manager. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords
- Unauthorised access to the CCG's systems either by staff or a third party.
- Unauthorised access to personal confidential data where the member of staff does not have a need to know.
- Disclosure of personal confidential data to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality.
- Sending personal confidential data or commercially sensitive data in a way that breaches confidentiality.
- Leaving personal confidential data lying around in public area.
- Theft or loss of confidential information.
- Personal confidential data or commercially sensitive found in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or Information Governance Manager staff should be sought.

Appendix 2: Summary of Legal and NHS Mandated Frameworks

The CCG is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the CCG who may be held personally accountable for any breaches of information security for which they may be held responsible. The CCGs shall comply with the following legislation and guidance as appropriate:

The **Data Protection Act (1998)** regulates the use of "personal data" and sets out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.
2. Processed for specified and lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and where necessary kept up to date.
5. Not kept longer than necessary, for the purpose(s) it is used.
6. Processed in accordance with the rights of the data subject under the Act.
7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data
8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

The Caldicott Principles should be applied when considering personal confidential data:

Principle 1 - Justify the purpose(s) of using confidential information

Principle 2 - Only use it when absolutely necessary

Principle 3 - Use the minimum that is required

Principle 4 - Access should be on a strict need-to-know basis

Principle 5 - Everyone must understand his or her responsibilities

Principle 6 - Understand and comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Article 8 of the **Human Rights Act (1998)** refers to an individual's "*right to respect for their private and family life, for their home and for their correspondence*". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

a. Making, supplying or obtaining articles for use in offences 1-3

The NHS Confidentiality Code of Practice (2003) outlines four main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

- Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

- Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to:
patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:
Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or
- We have special permission because the public good is thought to be of greater importance than your confidentiality, and
- If we share information without your permission, we will make sure that we keep to the Data Protection Act, the NHS Confidentiality Code of
- Practice and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the NHS understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.