NHS
Surrey Downs
Clinical Commissioning Group

Information Security Policy

Policy ID	IG03
Version:	1.1
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Executive Committee
Date agreed	27th January 2015
Next review date:	27th January 2017

Improving care together across Surrey Downs

EQUALITY STATEMENT

Surrey Downs Clinical Commissioning Group (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.

1. EQUALITY ANALYSIS

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

	Yes, No or N/A	Comments
1. Does the document/guidance affect one group less or more favourably than another on the basis of:		

	• Race	No	
	• 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?	N/A	
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	

For advice in respect of answering the above questions, please contact the Corporate Office, Surrey Downs CCG. If you have identified a potential discriminatory impact of this procedural document, please contact as above.

Names and Organisation of Individuals who carried out the Assessment	Date of the Assessment
Kate Taylor	May 2014
Justin Dix	

Information Security Policy

Contents

1. INTRODUCTION AND PURPOSE

Information security has critical importance to NHS patient care, information assets and other related business processes. High quality information underpins the delivery of high quality evidence-based healthcare. Without effective security, NHS information assets may become unreliable, may not be accessible when needed, or may be compromised by unauthorised third parties. Information, whether in paper or electronic form, is of high importance to the CCG, therefore the organisation must ensure that the information is properly protected and is reliably available.

Information security is primarily about people but is facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that the CCG is providing a secure and trusted environment for the management of information used in delivering its business.
- Clarity over the personal responsibilities around information security expected of staff when working on CCG business.
- A strengthened position in the event of any legal action that may be taken against the CCG (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.

2. SCOPE AND DEFINITIONS

2.1 SCOPE

This policy applies to all of the CCG's employees. Compliance and responsibility also extends to those employed as contractors, NHS professionals, temporary staff, voluntary organisations and anyone duly authorised to view or work with the CCG's information.

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient and staff records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. The CCG has a legal obligation to ensure that there is adequate provision for the security management of the information resources the organisation own, control, or use. This Information Security Policy forms part of a suite of Information Governance (IG) documentation including but not limited to: Information Governance Policy, Data Protection Act Policy, and the Records Management & Lifecycle Policy.

This Information Security Policy covers all forms of information held by the

CCG, including but not limited to:

- Information about members of the public and patients
- Non-CCG employees on CCG premises
- Staff and personnel Information
- Organisational, business and operational Information

This Information Security Policy applies to all aspects of information handling, including, but not limited to:

- Structured Record Systems – paper and electronic.
- Information Recording and Processing Systems – Paper, Electronic, Video, Photographic and Audio Recordings.
- Information Transmission Systems, such as fax, email, portable media, post and telephone.

2.2 DEFINITIONS

Asset
Anything that has value to the organisation, its business operations and its continuity.

Authentication
The organisation must ensure that the identity of a subject or resource is the one claimed.

Availability
The property of being accessible and usable upon demand by an authorised entity.

Business Impact
The result of an information security incident on business functions and the effect that a business interruption might have upon them.

Confidentiality
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Impact
The result of an information security incident, caused by threat, which affects assets.

Information Assurance
The confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

Information Security
The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability and reliability can also be involved.

Personal Confidential Data
This is where an individual can be identified from:
a) the data, or
b) from the data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (Data Protection Act 1998).

3. PROCESS REQUIREMENTS

This Information Security Policy will achieve a consistent approach to the security management of information throughout the CCG, and will aim to deliver continuous business capability, and minimise both the likelihood of occurrence and the impacts of information security incidents.

Security of our information is paramount and the protective measures put in place, must ensure that IG requirements are satisfied. The aim of this process is maintaining the confidentiality, integrity, and availability of the CCG's information. To conform to the Information Security Assurance requirements of Health & Social Care Information Centre IG Toolkit (IGT) the CCG shall:

Maintain the Confidentiality of Personal Information including patient and staff identifiable information by protecting it in accordance with NHS Information Security Code of Practice, Data Protection Act, Caldicott Principles and other legal and regulatory framework criteria.

Ensure the integrity of the CCG's information by developing, monitoring and maintaining it to a satisfactory level of quality for use within the relevant areas.

Implement the necessary measures to maintain availability of the CCG's information systems and services. This includes putting in place contingency measures to ensure the minimum of disruption caused to the CCG's information systems and services.

This Information Security Policy is consistent with and supports the CCG's policies and existing methods of working, which take precedence on any specific issue, and is in accordance with NHS national guidance.

3.1.1 Physical Security

The physical security of the CCG's information is the responsibility of all staff. The protection of both personal and non-personal information is paramount in maintaining confidentiality, and users of the CCG's information must comply with the suite of IG documentation. This is a local Information Security Policy to protect the information stored, processed and exchanged between the CCG and other organisations.

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause. Information security expectations of staff shall be included within appropriate job definitions.

Staff shall accept full responsibility for the security of information and information assets which are issued to them, taking necessary precautions to avoid loss, theft or damage. Information should not be left unattended in a public place or left in vehicles either on view, unattended or overnight. In the event of such an incident, staff must report this immediately to the NHS South East CSU IG team who will assist with the management of the incident.

All access to confidential and/or sensitive information (whether on paper or electronically) located within CCG property must be controlled through the use of the approved security measures. Advice and guidance can be sought from NHS South East CSU IG Team or the IT hosted service. Access to information shall be restricted to users who have an authorised business need and access has been approved by the relevant Information Asset Owner (IAO). Other staff responsibilities include ensuring perimeter security by making sure that security doors are closed properly, blinds drawn, and that any door entry codes are regularly changed.

All employees must wear identification badges. Individuals not wearing identification in areas which are not for public access should be challenged. Visitors should be met at reception points and accompanied at all times even when leaving the building.

Portable devices must not be used to store or transfer confidential information unless they are encrypted to an approved standard and comply with the Caldicott Principles. Employees on termination of employment or contract must surrender door keys, Smartcards and all other equipment provided by or belonging to the CCG.

Each team is responsible for holding an Information Asset Register which details the specification, user and location of the asset. IT equipment will be security marked and its serial number should be recorded. It is the responsibility of the area's assigned Data Custodian to update the asset register and submit to the NHS South East CSU IG Team. Each team will have a designated Information Asset Owner (IAO) who is responsible for all

information held and used by that team.

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed contracts with third party vendors working for and on behalf of the CCG to be in place.

3.1.2 Protection from Malicious Software

All IT equipment used by the CCG staff is protected by countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users are not permitted to install software on the organisation's property without permission from, at time of writing, the NHS South CSU Associate Director of ICT or the Information Security Officer. When this function moves to NHS South East CSU, that organisation's appropriate process must be followed. Users breaching this requirement may be subject to disciplinary action.

3.1.3 Preventing Information Security Breaches

Each CCG Team is responsible for regularly monitoring the information they hold and use. An annual mapping exercise of information flows in and out of the teams will be undertaken. This exercise will allow any information risks to be identified by each team and appropriate action to mitigate those risks should be taken. It is the responsibility of the IAO to ensure that this takes place.

Protection against unauthorised access or disclosure:

Staff have the responsibility to ensure that information is kept secure when being processed or transferred by adhering to the following:

- Screens should be locked when unattended even for short periods of time.
- Internet and email policies.
- Remote Working and Portable Devices Policy.
- Guidance provided on the use of fax, phones and post which can be found within the Safe Haven Policy.

For the secure transfer of bulk electronic information, secure file transfer function within NHSmail should be used as it has the approved levels of encryption.

The CCG will ensure that paper information is secure by following adequate records management procedures and processes. Staff should have access to secure storage areas and, if possible, a clear desk routine should be followed. Should a legitimate need arise for local storage or a non-routine transfer of confidential information then a risk assessment must be undertaken first and the justification approved by the Caldicott Guardian and recorded by the line manager. CCG staff must also ensure when moving

away from desks that they do not leave Personal Confidential Data / sensitive information available for others to view by putting it in a drawer or covering it up.

The CCG promotes a 'paperlite' environment through use of electronic devices to transform information to a secure electronic form.

Any non-routine bulk extracts (50+ records) or transfers of particularly confidential or sensitive data must be authorised by the responsible Director or the Information Asset Owner for the work area and may require approval by the Senior Information Risk Owner.

That the integrity and value of the information is maintained:

The organisation ensures that employees and contracted individuals are aware and apply the Data Protection Act and Caldicott Principles through their working practices. NHS South East CSU IG Team promotes the principles and provides or facilitates training.

That information shall be available to properly authorised personnel as and when it is required:

All employees are required to use the guidance contained in the NHS Confidentiality Code of Practice, Care Record Guarantee and the Records Management Code of Practice. The IG suite of policies provides further guidance.

Organisation-wide Business Continuity Plans for information systems are in place:

This includes identification and assessment of critical dependencies on the CCG's information resources. The organisation will implement a Business Continuity Management System (BCMS) that will be aligned to the international standard of best practice (ISO 22301 – Societal Security – Business Continuity Management Systems). Business Impact Analysis will be undertaken in all areas of the organisation.

Business Continuity Plans will be put into place to ensure the continuity of prioritised activities in the event of a significant or major incident. The SIRO has a responsibility to ensure that appropriate Disaster Recovery Plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis.

Relevant Information Security Training and awareness is available to staff:

This is delivered via the Health and Social Care Information Centre (HSCIC) IG Training Tool (IGTT). Additional training needs beyond this will be

assessed.

All breaches of information security, actual or suspected, are recorded:

Incidents must be reported using the agreed incident management process for the CCG.

3.1.4 Potential or Actual Information Security Breaches

All staff are responsible for ensuring that no potential or actual security breaches occur as a result of their actions. NHS South East CSU IG Team will investigate all suspected / actual security breaches.

NHS South East CSU IG Team CCG Risk Lead must be informed of all security issues in order to ensure that the appropriate investigations are carried out. The appropriate NHS South East CSU Registration Authority (RA) Manager will also receive copies of any Registration Authority related security breaches or incidents.

Depending on the impact of the incident, external organisations such as the NHS England, HSCIC and the Information Commissioners Office may need to be informed.

The resulting Root Cause Analysis (RCA) report will specify, details of suspected incident, assets affected or compromised and investigation conducted. Recovery/contingency plans, damage and risk classification and recommendations will be provided.

All incidents will be investigated immediately and reported in a timescale appropriate to the initial risk assessment. Reports and recommendations will be approved and monitored by an appropriate Group the CCG.

3.1.5 Risk

The CCG will need to ensure that adequate audit provision is in place to ensure continuing effectiveness of information security management arrangements.

Any security measures must be viewed as necessary protection against a risk of an event occurring or to reduce the impact of such an event. Some of these events may be deliberate acts of damage and others may be accidental. Nevertheless, a range of security measures can be deployed to address:

- The **Threat** of something damaging the confidentiality, integrity or availability of information held on systems or manual records.
- The **Impact** that such a threat would have if it occurred.
- The **Likelihood** of such a threat occurring.

All staff should consider the risks associated with the computers they use and the information that is held on them, as well as information held in manual records

All staff are responsible for reporting any apparent shortcomings of security measures currently employed to address these risks to the risk lead within the CCG.

3.1.6 Information Disposal

Electronic

Computer assets must be disposed of in accordance with the ICT Provider disposal of confidential waste procedure. This includes removable computer media, such as tapes and disks.

All data storage devices must be purged of sensitive data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider. For further information, please contact the CCG's hosted IT provider.

Paper

Printed matter should be confidentially destroyed using an appropriate method such as shredding. Where the CCG has large quantities of confidential waste which need to be disposed of the CSU IG team can help facilitate this through a secure shredding contract.

3.1.7 Security of Third Party Access to NHS Networks

Written agreement must be received from all external contractors and non-NHS parties that they agree to treat all information confidentially and that information will not be disclosed to unauthorised individuals. Such contractors should also sign a declaration that they understand the relevant legislation should they need to access sensitive information stored on a computer system. This declaration is available at appendix 2

4. ROLES AND RESPONSIBILITIES

The Accountable Officer has overall responsibility for governance within the organisation. As the 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.

The Caldicott Guardian is seen as the 'conscience' of the organisation regarding the use of personal confidential data. They are responsible for ensuring all personal confidential data is shared in an appropriate and secure manner.

The Senior Information Risk Owner (SIRO) is responsible for providing leadership on the management of 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 Executive Management Team is adequately briefed on information risk issues. The joint CCG and CSU IG team will support this role.

The Information Security Expert is responsible for the implementation and enforcement of information security. Regular reports will be submitted to the CCG's Executive Committee.

Information Asset Owners (IAO) in each department support the SIRO; their role of IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The organisation has allocated this role to Senior Departmental Heads and/or Managers for each department.

Data Custodians have the responsibility of assisting the IAOs in providing assurance that information risk and the handling of information requirements are managed effectively. Data Custodians should also ensure staff compliance with policies and legislation/principles (Data Protection Act 1998, Common Law Duty of Confidentiality and Caldicott principles).

The CCG will ensure that applications to use remote working systems, portable computing and data storage resources, are approved via an agreed process that can be audited.

All employees, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of the legal and policy requirements incumbent upon them and for ensuring that they comply with these on a day-to-day basis.

All staff must abide by this and associated policies and procedures.

All staff should report any suspected breaches of this policy to their line manager or the assigned Data Custodian and the NHS South East CSU IG team.

All staff must be aware and understand that failure to comply with the rules regulations contained within this policy, may result in disciplinary action.

5. TRAINING

The CCG recognises that staff are working to a code of conduct which stresses the importance of appropriate information handling which incorporates statutory, common law and best practice requirements. As IG is a framework drawing these requirements together, it is important that staff receive the appropriate training.

The NHS Operating Framework 'Informatics Planning' requires that the organisation ensures all staff receives annual basic IG training appropriate to their role through HSCIC IGTT. Managers are responsible for monitoring staff compliance.

CCG staff also receive an IG Staff Handbook on joining the organisation.

All staff are required to undertake IG Training annually via the IGTT.

6. EQUALITY AND DIVERSITY

This policy was assessed against the CCG's Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity issues this can be seen at appendix 1.

7. SUCCESS CRITERIA/MONITORING OF THE EFFECTIVENESS OF THE POLICY

The CCGs IG Steering Group is responsible for the approval of this policy. The Management Committee will then ratify that approval.

NHS Surrey Downs CCG's Senior Information Risk Owner (SIRO), Information Asset Owners and Data Custodians are responsible for the implementation of this policy throughout the organisation.

Regular audits should be undertaken by Data Custodians to ensure that all portable computing and mobile devices issued can be accounted for and that assurance is provided to the Senior Information Risk Owner (SIRO) that identified risks are adequately controlled and managed.

Adherence to this policy will be monitored via investigation and analysis of information security incidents reported via the approved incident management process.

8. REVIEW

The CCG Executive Management Team is responsible for the review of this policy.

9. REFERENCES AND LINKS TO OTHER DOCUMENTS

Information Governance Policy
Information Governance Framework
Data Protection Policy
Safe Haven Policy
Information Security Management: NHS Code of Practice
NHS Records Management: Code of Practice
NHS England Information Security Policy

APPENDIX 1

Confidentiality agreement – NHS South Commissioning Support Unit

Document name	NHS Surrey Downs CCG Confidentiality Agreement
Date:	03/02/2012
Author	NHS Surrey Downs Clinical Commissioning Group
Version	1

Confidentiality agreement for third party suppliers

WHO ARE THIRD PARTIES COVERED BY THIS AGREEMENT?

Third party suppliers granted access to NHS Surrey Downs Clinical Commissioning Group data and information in order to perform tasks as required by NHS Surrey Downs Clinical Commissioning Group. They could include the following:

- Hardware and software maintenance and support staff (for all of the document)
- Cleaning, catering, security guards and other outsourced support services (for general contractor clause and form on back page)

GENERAL CONTRACTOR CLAUSE

(Based on clause from Introduction to Data Protection in the NHS.)

The Contractor undertakes:

- To treat as confidential all information which may be derived from or be obtained in the course of the contract or which may come into the possession of the contractor or an employee, servant or agent or sub-contractor of the contractor as a result or in connection with the contract; and
- To provide all necessary precautions to ensure that all such information is treated as confidential by the contractor, his employees, servants, agents or sub-contractors; and
- To ensure that they, their employees, servants, agents and sub-contractors are aware of the provisions of the Data Protection Act 1998 and ISO/IEC 27002 and that any personal information obtained from the CCG shall not be disclosed or used in any unlawful manner; and
- To indemnify the CCG against any loss arising under the Data Protection Act 1998 caused by any action, authorised or unauthorised, taken by himself, his employees, servants, agents or sub-contractors.

All employees, servants, agents and/or sub-contractors of the Contractor will be required to agree to and sign a confidentiality statement when they come to any of the CCG sites where they may see or have access to confidential personal and/or business information (see last page).

SUPPLIER CODE OF PRACTICE

The following Code of Practice applies where access is obtained to CCG information for the fulfilment of a required service.

The access referred to in paragraph 1 above may include:-

- Access to data/information on the CCG premises
- Access to data/information from a remote site
- Examination, testing and repair of media (e.g. fixed disc assemblies)
- Examination of software dumps
- Processing using CCG data/information

The Supplier must certify that his organisation is registered if appropriate under the Data Protection Act 1998 and legally entitled to undertake the work proposed.

The Supplier must undertake not to transfer any personal data/information out of the European Economic Area (EEA) unless such a transfer has been registered, approved by the CCG and complies with the Information Commissioners guidance on Safe Harbours.

The work shall be done only by authorised employees, servants, or agents of the contractor (except as provided in paragraph 12 below) who are aware of the requirements of the Data Protection Act 1998 of their personal responsibilities under the Act to maintain the security of the CCGs personal data/information.

While the data/information is in the custody of the contractor it shall be kept in appropriately secure means.

Any data/information sent from one place to another by or for the contractor shall be carried out by secure means. These places should be within the suppliers own organisation or an approved sub-contractor.

Data/Information which can identify any patient/employee of the CCG must only be transferred electronically if previously agreed by the organisation. This is essential to ensure compliance with strict NHS controls surrounding the electronic transfer of identifiable personal data/information and hence compliance with the Data Protection Act 1998 and BS7799. This will also apply to any direct-dial access to a computer held database by the supplier or their agent.

The data/information must not be copied for any other purpose than that agreed by the supplier and the CCG.

Where personal data/information is recorded in any intelligible form, it shall either be returned to the CCG on completion of the work or disposed of by secure means and a certificate of secure disposal shall be issued to the organisation.

Where the contractor sub-contracts any work for the purposes in paragraph 1 above, the contractor shall require the sub-contractor to observe the standards set out in this agreement.

The CCG shall, wherever practical, arrange for the equipment or software to be maintained, repaired or tested using dummy data that does not include the disclosure of any personal data/information.

The CCG reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The CCG will expect an escalation process for problem resolving relating to any breaches of security and/or confidentiality of personal information by the suppliers employee and/or any agents and/or sub-contractors.

Any security breaches made by the supplier's employees, agents or sub-contractors will immediately be reported to the CCG Caldicott Guardian.

Certification form:

NAME OF SUPPLIER:	
ADDRESS OF SUPPLIER PRIME CONTRACTOR:	
TELEPHONE NUMBER:	
EMAIL DETAILS:	

On behalf of the above organisation I certify as follows:

The organisation is appropriately registered under the Data Protection Act 1998 and is legally entitled to undertake the work agreed in the contract agreed with the Organisation

The organisation will abide by the requirements set out above for handling any of the organisation personal data/information disclosed to my organisation during the performance of such contracts

SIGNED:	
NAME OF INDIVIDUAL:	
POSITION IN ORGANISATION:	
DATE:	

Agreement outlining personal responsibility concerning security and confidentiality of information (relating to patients, staff and the business of the organisation)

During the course of your time within the CCG buildings, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties as detailed in the contract between the CCG and your employer. This condition applies during your time within the CCG and after that ceases.

Confidential information includes all information relating to the business of the CCG and its patients and employees.

The Data Protection Act 1998 regulates the use of all personal information and included electronic and paper records of identifiable individuals (patients and staff). The CCG is registered in accordance with this legislation. If you are found to have used any information you have seen or heard whilst working within the CCG for any other purpose than that which it was shared with you both you and your employer may face legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to the conditions within the Contract between the organisations and my personal responsibilities to comply with the requirements of the Data Protection Act 1998.

NAME OF ORGANISATION:	
CONTRACT DETAILS:	
PRINT NAME:	
SIGNATURE:	
DATE:	

END OF DOCUMENT