NHS
Surrey Downs
Clinical Commissioning Group

Information Governance Staff Handbook

November 2016 v5.3

Improving care together across Surrey Downs

Contents

1 Introduction 3
2 Legislation and regulations 3
3 Information Governance structure 4
4 Caldicott principles and Data Protection Act principles 5
5 Guide to confidentiality 6
6 Reporting possible breaches of security or confidentiality 11
7 Monitoring access to personal confidential data and sensitive information 11
8 IT security 11
9 Remote working and portable devices 12
10 Information Governance mandatory training 13
11 Records management 13
12 What to do in the event of missing corporate or health records 15
13 Freedom of Information 15
14 Business continuity plans 17
15 Information sharing 17
16 Smartcards 18
17 Key Information Governance contacts 19
18 Confirm you have read and understand this IG Staff Handbook 19
Information Governance staff handbook confirmation slip 20

1 Introduction

Information Governance (IG) is the practice used by all organisations to ensure that information is efficiently managed and that appropriate policies, system processes and effective management accountability provides a robust governance framework for safeguarding information.

Information Governance enables organisations to embed policies and processes to ensure that personal and sensitive information is:

- Held securely and confidentially;
- Obtained fairly and efficiently;
- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared appropriately and lawfully.

NHS organisations hold numerous amounts of personal and sensitive information, and all staff should be able to provide assurance that the Information Governance standards are incorporated within their working practices.

Personal and sensitive information can be contained within a variety of documents. For example:

- Health Records;
- Staff Information;
- Corporate Information;
- Commissioning Information;

It is important for staff to be aware of what constitutes personal and sensitive information. Further details on types of information are available within the Confidentiality module on the Health and Social Care Information Centre (HSCIC) – Information Governance Training Tool.

2 Legislation and regulations

Members of staff should also be aware of the legislation surrounding Information Governance that stipulate how organisations should safeguard information, what processes are in place to use, secure and transfer information and also how patients and members of public have access to personal/business information. The organisation must comply with the following:

- Data Protection Act 1998
- Caldicott Principles and Caldicott 2 Review
- Freedom of Information Act 2000
- Privacy and Electronic Communications
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Common Law Duty of Confidentiality

The CCG have produced a suite of policies, processes and procedures, which can be found on the staff intranet.

Adherence to information governance principles ensures compliance with the law, best practice and embeds processes that help staff manage personal confidential and sensitive information appropriately. It must also be noted that embedding information governance processes enables patients and service users to have greater trust in the CCG and enables effective working across partner organisations.

3 Information Governance structure

Accountable Officer

The CCG Accountable Officer has overall responsibility for IG within the organisation. As Accountable Officer, they are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

Senior Information Risk Owner

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

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 a clinical background. The IGSG supports the Caldicott Guardian in fulfilling his role.

The Caldicott Guardian has particular responsibilities for ensuring that the organisation is protecting the confidentiality of patients/service-user's information and enabling appropriate information sharing. Acting as the 'conscience' of the organisations, the Caldicott Guardians 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.

Information Asset Owners (IAOs)

The SIRO is supported by Information Asset Owner (IAOs). The role of IAOs 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 IGSG supports the IAOs in fulfilling their role.

Data Custodians

IAOs 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

4 Caldicott principles and Data Protection Act principles

The Caldicott Principles

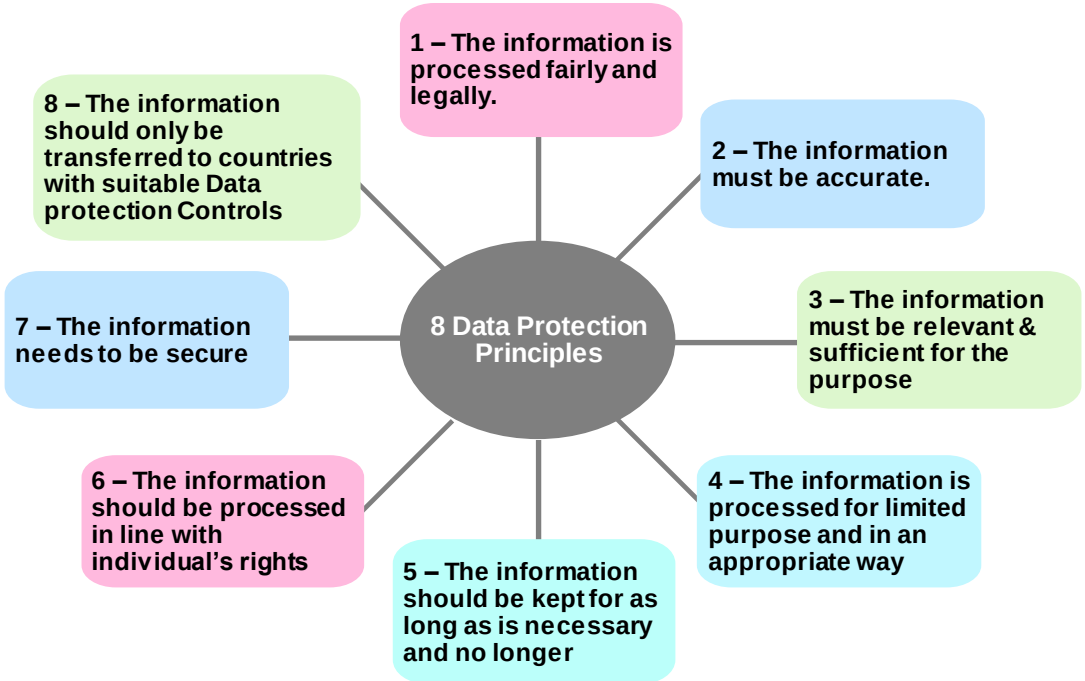
The Caldicott committee makes recommendations aimed at improving the way the NHS uses and protects confidential information. All NHS employees must be aware of the seven Caldicott Principles which apply to both patient and personnel data.

Principle 1:	Justify the purpose - Why is the information needed
Principle 2:	Don't use patient identifiable information unless absolutely necessary – Can the task be carried out without identifiable information?
Principle 3:	Use the minimum necessary patient identifiable information – Can the task be carried out with less information?
Principle 4:	Access to patient identifiable information should be restricted to required/relevant personnel.
Principle 5:	Everyone with access to patient identifiable information should be aware of their responsibilities – Lack of knowledge is not acceptable
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.

Data Protection Act 1998 and the Data Protection Act principles

All organisations in the country must comply with the Data Protection Act 1998. Data protection law is enforced in the UK by the Information Commissioner's Office (ICO) and has the power to fine organisations up to £500,000 for data protection breaches.

The following is the eight Data Protection Act principles that must be followed when handling personal and sensitive information. These principles should be considered when handling both corporate and clinical records.



5 Guide to confidentiality

Everyone working in or for the NHS has the responsibility to use personal data in a secure and confidential way. Staff who have access to information about individuals (whether patients, staff or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This guide sets out the key principles and main 'do's and don'ts' that everyone should follow to achieve this for both electronic and paper records.

The common law of duty of confidentiality requires that information that has been provided in confidence may be disclosed only for the purposes that the subject has been informed about and has consented to, unless there is a statutory or court order requirement to do otherwise.

Personal Confidential Data is information about any living individual who can be identified from that data, such as, patient's health care professionals, other staff, and suppliers, contractors etc. Such person-identifiable information may be manually-held or automated and includes for example, the contents of filing cabinets, all patient information, including medical records, photographs, x-rays, and other images, computer disks, tapes, CD ROMs etc. Personnel records include those held by line managers, as well as, those held centrally by personnel departments. The use of all such personal data is controlled by the eight data protection principles. The Access to Health Records Act 1990 was largely superseded by the Data Protection Act 1998, but still applies to the records of deceased persons.

These Caldicott and Data Protection principles translate into **key maxims for all staff to follow:**

- Patients and staff should be fully informed about how their information may be used.
- There are strict conditions under which personal data may be disclosed.
- In particular, certain disclosures are not allowed without the express consent of the individual.
- Individuals have the right to see what information is held about them, and to have any errors corrected. They also have the right to request copies.
- Personal information should be anonymised wherever and whenever possible.
- The legitimate use, disclosure or sharing of personal data does not constitute a breach of confidentiality.
- Sharing of personal data between organisations can take place with appropriate safeguards.
- Sometimes a judgement has to be made about the balance between the duty of confidence and disclosure in the public interest. Any such disclosure must be justified.
- Personal data should be kept secure and confidential at all times – as detailed below.

Under **current legislation** commissioners can only process or have access to personal confidential data if one of the following criteria is satisfied:

- Consent has been obtained from the individual.
- There is a legal basis for the use of the data e.g. Section 251 for Risk Stratification, Controlled Environment for Finance (CEfF) and Accredited Safe Haven (ASH)
- The data has been anonymised.
- The data is held in respect of safety, safeguarding or in the public interest; any such decision taken to share personal confidential data as a result of the above should be documented and agreed by the SIRO and Caldicott Guardian

Section 60 of the Health and Social Care Act as re-enacted by **Section 251 of the NHS Act 2006** allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. The Regulations that enable this power are called the Health Service (Control of Patient Information) Regulations 2002. Any references to 'section 251 support or approval' actually refers to approval given under the authority of the Regulation

Controlled Environment for Finance (CEfF) allows CCG and CSUs to process Personal Confidential Data (PCD) which are required for invoice validation purposes under the section 251 agreement.

Accredited Safe Havens (ASH) are an accredited organisation with a secure electronic environment in which personal confidential data and/or weakly pseudonymised data can be obtained and made available to users, generally in de-identified form. An accredited safe haven will need a secure legal basis to hold and process personal confidential data. Weakly pseudonymised data can be held under contract with obligations to safeguard the data. The South East CSU Information Governance Subject Matter Expert (IG SME) can advise on the ASH arrangements for the CCG.

Staff should check with the IG SME or a member of the IGSG if they have any queries on whether to access or process personal confidential data

Some of the ways to keep information secure and confidential are:

1. Organisational arrangements

Make sure you know the name of the following in your team or for the organisation as a whole:

- SIRO
- IG Service Lead/ SME
- Caldicott Guardian
- Data Custodian
- IAO

2. Limiting unnecessary access to personal information

- Do not discuss confidential matters outside of work, or even with anyone at work who does not need to know it; be aware that other people may overhear.
- Do not leave working papers lying around the office, or put confidential items exposed in in-trays; remove documents from photocopiers and fax machines as soon as possible after use.
- Hold keys and other access means, such as combination of locks, securely away from the point of storage when not in use. Ensure that there is an appropriately secure system in place to allow access in event of emergency or an individual's absence.
- Keep offices locked when unoccupied, and maintain overall building security.
- Keep workstations and other computer equipment secure, being particularly careful with laptops when not in use, especially not leaving them unattended in cars.
- Lock away portable devices when not in use.
- Do not write down your computer passwords or share them with anyone.
- Ensure that your PC monitor screen cannot be seen by other people, being careful in public reception areas. Security Screens should be used where needed.

- Do not leave your PC unattended whilst it is logged-in to the network or any system. Lock your screen every time you leave your desk.

3. Ensuring authorised access only

- Access to records will be on a 'need to know' basis only.
- There is no automatic right of access to records and access must be agreed in advance with the Data Custodian or data 'owner'. This can be either verbal or written permission.

4. Accuracy, retention and disposal

- If adding information to records, ensure accuracy and relevance; any queries should be raised with the Information Asset Owner
- If you are an 'Information Asset Owner' ensure that records are held with informed consent, are relevant for the purpose held, and are kept accurate and up – to – date; ensure that records are archived yearly and held no longer than necessary for their purpose and in accordance with the NHS mandatory Retention and Disposal Schedule.
- Ensure any personal or sensitive information is confidentially destroyed in accordance with the CCG's Information Security policy. (Note that ordinary waste bins and 'recycling' bins are not to be used for papers showing personal or otherwise confidential details).
- Dispose of redundant equipment, especially disc or tape copies of confidential or sensitive information, in the proper manner through the CCG's ICT Service Provider – South East Commissioning Support Unit (the CSU).

5. Off-site working

- Do not take records or other confidential information out of the office and especially off-site unless authorised.
- Always make sure that a list of the records that you take off site is retained at your base.
- Protect the security and confidentiality of the information at all times. If records are taken off-site by agreement, they should be transported out of site in the boot of the car and removed to a place of safety on arrival at your destination.

6. Requests for information

If you receive a request for information about a patient, staff member, etc. and it is not usually part of your job to respond refer to the Subject Access Request section.

7. Abuse of privilege

- Do not pass any information to your own relatives or friends, and do not attempt to find out details about them.
- Do not pass on any information for personal or commercial gain.
- Do not attempt to access your own records unless through the appropriate procedure.

8. Disclosures

You may, as part of your job, need to disclose patient information to others:

- Keep the amount of information disclosed (even within the NHS) to the minimum necessary.
- Do not duplicate records, (on paper, or in a computer) unless essential for the purpose.

9. Patient contacts and patient details

- Do not leave messages that contain personal or sensitive information on home answering machines as it may not be the person for whom the message is intended for.
- White boards or other displays that contain personal or confidential information should not be visible to the public.
- Any notes containing personal data written whilst taking a phone call or other message should be confidentially destroyed.

10. Transferring personal confidential or sensitive information

The Information Commissioner's Office (ICO) has reported that there has been a number of insecure transfers of information via fax, post and emails and has imposed monetary penalties on organisations who have failed to comply with the **Data Protection Act**. In order to prevent this occurring within the CCG, it is the responsibility of each individual member of staff to ensure that the following processes are followed when transferring personal identifiable and sensitive information.

11. NHSmail process:

It is policy that emails containing any PCD or commercially sensitive information should be sent using an NHS.net account. Any PCD sent by this method is secure as long as it is sent to one of the following type of email accounts:

Another NHS.net account

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

If you intend to send personal or sensitive information to any other type of email account not listed above, the information should be sent as an encrypted attachment. Do not include PCD in the subject header when sending an e-mail. Please seek advice from CCG IG Manager or member of the IGSG.

12. Safe Haven fax process

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so or when an alternative secure method is not available. 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.
- Telephone the recipient when you are sending the fax and ask them to return the call to acknowledge receipt and number of pages.
- 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.
- 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 dialling incorrect numbers.
- 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 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.

13. Safe Haven post process:

- 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 or sensitive information.
- Ensure post is sent to a named person and clearly addressed.
- A return address should be shown on all post.
- Staff sending documents by external post or courier, use a 'signed for' delivery service. PCD should be sent by Special Delivery. 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'.
- Consider carrying out a risk assessment if appropriate.

14. Subject Access Requests (SARs)

Under the Data Protection Act 1998, all living individuals or 'Data Subjects' have a right to be informed of the following:

- If the CCG holds, stores or processes personal data about them.
- A description of the Personal Data held, the purposes for which it is processed and to whom the personal data may be disclosed.
- A copy of any information held.
- To be informed as to the source of the data held.

The CCG's Head of Human (HR) is responsible for ensuring that SARs relating to staff are effectively managed, systems and procedures are in place to support access to records across the organisation. The CCG's Continuing Health Care (CHC) Business Manager is responsible for processing SARs relating to patients/service-users.

All staff have a responsibility to ensure they support with the subject access request process for the CCG.

For further guidance on SAR please see document on Subject Access Requests Procedures on the CCG website.

6 Reporting possible breaches of security or confidentiality

Since April 2010, the ICO is able to issue monetary penalties to any organisation found to be in breach of the Data Protection Act. A fine of up to £500,000 may be incurred for a serious breach. The ICO can also conduct an investigation into less serious breaches which can lead to an organisation having an enforcement notice/undertaking imposed upon them.

The ICO may impose the monetary penalty notice if the organisation has seriously breached the Data Protection Act principles:

- Which likely to have caused substantial damage or distress.
- Was deliberate or the organisation must have known or ought to have known that there was a risk that a breach would occur and failed to take reasonable steps to prevent it.

Each member of staff has the responsibility to ensure that information is handled, stored and transferred in a safe, secure and appropriate way. Members of staff should always:

- Report any incident that could possibly relate to a breach of confidentiality, e.g. the loss, theft or corruption of information, a network security breach, loss or theft of a computer, password misuse, etc.
- Think carefully before sharing PCD without explicit consent, as staff may be held accountable for any unauthorised disclosure.
- Do not open suspicious e-mails. Report any possible IG or cyber incidents to the CCG's IG Manager or a member of the IGSG.

For further guidance on incident reporting, please refer to the CCG's published corporate and information governance policies on the CCG web site.

7 Monitoring access to personal confidential data and sensitive information

Staff members should be aware that electronic systems access, process or transfer PCD are monitored on a continuous basis. Any breach of security or infringement of confidentiality may be regarded as serious misconduct, which would lead to disciplinary action or dismissal in accordance with disciplinary procedures. In addition, unauthorised disclosure of personal information is an offence and could lead to prosecution of individuals and/or the organisation.

8 IT security

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.

- Access to all CCG confidential or sensitive information whether held on paper or electronically must be restricted.
- Staff must ensure that doors and windows are closed properly, blinds drawn, and that any door entry codes are changed regularly, ideally when a member of staff leaves the team or it is suspected that someone else knows the code.
- All employees should wear identification badges and where practical should challenge individuals not wearing identification in areas they know are not for public access. Visitors should be met at reception points and accompanied to appropriate member of staff or meeting and also should be asked to sign in and out of the building.

- Employees on termination of employment or contract must surrender door keys, Smartcards and all relevant CCG equipment in compliance with the CCG leavers' process.
- All computer assets including hardware and software must be recorded on an asset register that details the specification, user and location of the asset.

All staff are responsible for ensuring that no actual or potential security breaches occur as a result of their actions. The organisation will investigate all suspected and actual security breaches.

9 Remote working and portable devices

The developments with information technology have enabled staff to adapt to more flexible and effective working practices, by providing mobile computing and portable devices. Although these working practices are advantageous, it is important for all staff to understand the associated risks to the information, and the responsibility to ensure that information accessed remotely or held on portable devices, is protected by adequate security.

It is important for staff to protect information which is processed remotely or is stored on portable devices and staff should read relevant CCG policies to ensure good practice.

Staff are responsible for the security of any portable devices issued to them, and should take all necessary precautions to avoid loss, theft or damage. In the event of loss, damage or theft occurring, they must report this immediately to their line manager and ICT service desk. Staff should also complete the CCG's Incident Reporting form and submit a copy to the South East CSU's Information Governance Compliance Officer (IG CO).

For further guidance on incident reporting, please refer to the Information Governance and Cyber Security Incident Management and Reporting Procedures on the CCG website.

Remote working and portable devices best practice guidance

- Encryption is mandatory in all mobile devices used to store identifiable data.
- Any portable computing device must not be left unattended in a public place or left in vehicles either on view, unattended or overnight. When transporting it, ensure that it is safely stored out of sight.
- Staff should take extra vigilance if using any portable computing device during journeys on public transport to avoid the risk of theft of the device or unauthorised disclosure of the organisation's stored information by a third party "overlooking". There are security measures which can be deployed to support this if such travel is common to the role, staff should enquire through their line managers.
- Staff should not leave the device unattended for any reason unless the session is "locked" and it is in a safe working place, devices should not be left in an unattended publically accessible room for example. If possible staff should take the device with them.
- Ensure that other 'non' authorised users are not given access to the device or the data it contains.

Passwords and PIN codes

- Passwords should be a combination of letters and digits of a pre-determined length and combination of characters, typically using the lower case of the keyboard.
- Passwords and/or PINs should not normally be written down, but if unavoidable, should be held on your secure drive in a passwords folder and never kept with the device or in an easily recognisable form.

Portable computing devices

- Sensitive corporate and PCD must not be stored or transferred using any unencrypted “USB Memory” device.
- Where it is not possible to encrypt sensitive/personal information, the advice of the IG Manager should be sought and, a one off data transfer solution should be found using a secure method.
- Portable devices should only be used to transport confidential or sensitive information when other more secure methods are not available.
- Information should not be stored permanently on portable devices. Always transfer documents back to their normal storage area as soon as possible.
- Staff must ensure that any suspected or actual breaches of security are reported to their line manager.
- Staff must ensure that the mobile devices are used appropriately at all times.
- Staff should not under any circumstances use any mobile device whilst in control of a vehicle.
- All staff should be aware of their surroundings when using a mobile device, especially when discussing confidential information.

10 Information Governance mandatory training

Every individual who works for the organisation is required to complete mandatory annual IG training. This includes all new starters, existing and temporary members of staff, and contractors. The CCG has a responsibility to ensure that those working with our information are aware of the IG principles and the risks to the reputation of our CCG which may occur, if processes are not followed.

All staff are required to complete training either through the HSCIC Training Tool or specially organised face-to-face sessions.

The CCG has in place Training Needs Analysis (TNA) document that identifies IG training modules for various job roles and functions.

All new starters, temporary staff and contractors working will need to complete the ‘Introduction to Information Governance’ module. Existing staff that have already completed the ‘Introduction to Information Governance’ should then complete the Information Governance Refreshers module for subsequent years. However, existing staff can complete the introductory modules should they need more in-depth IG training.

The link to the IG Training Tool has recently been changed and can now be accessed via the following link https://www.igtt.hscic.gov.uk/igte/index.cfm.

11 Records management

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal. It is the aims of the organisation to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

The NHS has two categories of records, health and corporate.

Health records can be considered records which contain all patient health records for all specialties, and including private patients, such as x-ray and imaging reports, registers, etc.

Corporate Records can be considered records which contain all administrative records, e.g. personnel, estates, financial and accounting records, notes associated with complaints.

Records within the NHS can be held in paper/manual or electronic format and as the National Care Record service is now implemented, all NHS organisations will have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Record Guarantee.

Corporate records

Records are the corporate memory of an organisation. Records are a fundamental corporate asset and are required to provide evidence of actions and decisions, enabling the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the Data Protection Act 1998 and the Freedom of Information Act 2000.

Corporate records also support strategic decision making enabling the organisation to protect the interests of staff, patients, public and other stakeholders.

Corporate records should:

- be accurate and complete
- be arranged systematically
- should be sufficient to enable other members of staff to carry out their tasks
- demonstrate compliance with legal and regulatory requirements.

Paper (manual) records

- A uniform filing system should be implemented to ensure that documents are grouped appropriately and consistently. Records that are frequently used should be stored within secure filing cabinets or secure areas (locked rooms, coded areas). Infrequently used records should be archived in secure rooms. If records are no longer needed and do not need to be kept according to the retention timeframes, the records should be confidentially destroyed.
- The filing system should also be kept simple and easy for all to understand.
- It should also be discussed with line management whether records are to be kept manually or electronically. This will help determine the definitive record.
- Paper files should be labelled accurately and clearly. Labels should be brief, have a meaningful description of the contents, and intelligible to both current and future members of staff.
- Where appropriate, templates should be used.
- Version controls should be applied and periodically reviewed.
- All paper files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived or destroyed. It would be useful to have a tracker card or spreadsheet to include who uses the file, location of where the file is situated and also retention review date.
- Should the file contain PCD, it is important not to add this to the title of the record and should be kept in a secure location. Page numbering confidential files will confirm if pages have been removed or are missing.

- Permission to access PCD should be restricted to a limited number of staff who require access.
- Records should be reviewed on a periodic basis to ensure that destruction rules apply.
- Annual confidentiality audits will be carried out by the Data Custodian for each service and results shared with service leads.

Electronic records

- Electronic files should be named accurately, simply and be easy for all to understand. A file structure should be used to ensure that all members of staff can follow the same filing structure.
- It is best to restrict 'creating or deleting folder responsibility' to limited amount of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to granted permission from the lead administrator.
- All electronic files should be reviewed at the end of every financial year. This will identify if records need to be retained.
- Each department/directorate should compile a list of standard terms and uniform terminology as naming conventions for files and folders.
- Version controls should be applied and periodically reviewed.
- Records with PCD should be controlled through the use of logins, password protection and encryption. Please review the CCG's Information Security Policy.

12 What to do in the event of missing corporate or health records

Missing records are a serious risk to the organisation and it is therefore vital that a tracing procedure is undertaken. Should records go 'missing' the following procedures should be followed:

1. Highlight the fact that a record is 'missing' to the Information Asset Owner (IAO) and work colleagues as soon as this becomes apparent.
2. Search in the place you would normally expect to see the record but look either side and above and below where it should be filed (should the record be manual). Search in other folders or conduct a 'search' within your files (should the record be electronic)
3. Should the record remain missing after your search, you will need to contact the IG Manager
4. Relevant staff should be made aware of the name of the record that is missing.
5. The IG Manager will inform CCG's Senior Information Risk Owner (SIRO) and Caldicott Guardian of the loss and advice on the level of the information risk.
6. Consideration will then be given as to whether the loss needs to be reported to the Information Commissioner's Office.

13 Freedom of Information

The Freedom of Information Act 2000 (FOIA) encourages transparency within the public sector and assumes that openness is standard so that, for example, decisions on how public money is spent or services provided can be seen and understood.

How to identify a Freedom of Information request

Any member of the public can ask to see information that is held by the CCG and any member of staff may be approached and asked for information under the FOIA.

The law requires the CCG to respond within 20 working days of receipt and staff need, therefore, to be alert to any requests received to ensure they are processed promptly and appropriately.

The FOIA gives a right of access to information and does not require justification or the reason behind the request to be provided by the requestor.

ALL staff have a duty to:

1. Recognise requests made under FOI;

Enquirers do not have to mention the term FOIA so consider this if the request does not fall into one of the following categories:

- A solicitor's letter
- A complaint
- A request for access to personal records
- A press enquiry
- Research
- A routine enquiry which can be responded to as "business as usual" i.e. advice, leaflets, contact details etc.

2. Provide help and advice to applicants:

- Direct all requests to the Freedom of Information Lead for action
- Advise applicants that the request must be written (email is acceptable) and includes a name and contact address; help them put their request in writing if necessary
- Direct requesters to the online Publication Scheme if it is known the information requested can be sourced there
- Advise there are a number of exemptions within the FOIA under which the CCG may not be obliged to provide the information requested
- Advise that a fee may be applicable, depending on the type and size of the request

3. Requests for information you may hold

The CCG, its staff and hosted organisations are obliged to respond to requests; failure to comply with the FOIA has legal implications not only for the CCG but for each individual member of staff. More detailed advice is held please refer to the CCG FOI Policy.

Under the FOIA all types of recorded information can be requested and may be disclosed, including everything written in notebooks or on "Post It" notes as well as your formal paper and electronic records. Very little information is "exempt" – this is only applicable where the public interest is best served by non-disclosure.

All FOI requests should be immediately passed to the communications team or emailed to foi@surreydownsccg.nhs.uk .If you have any questions or are not sure whether the communication is an FOI request please contact the communications team for advice.

4. New or existing programmes and projects

It is the responsibility of all staff to incorporate information governance into their working practices and to also make partner organisations provide assurance that information will be handled in a secure and appropriate manner. As part of the Information Governance framework, we ask staff to consider IG implications when starting new projects and programmes. It is important to involve the IG CO at Programme and Project initiation stage to advise of the IG elements which will need to be considered. A Privacy Impact Assessment (PIA) is a tool used by to help establish Information Governance implications at the start of a programme and project.

Identifying information governance elements at an early stage will ensure;

- Compliant operations;
- Necessary information sharing protocols are put in place,
- The CSU is aware of and can effectively monitor data

It will also eliminate the potential of failing to comply with the Data Protection Act 1998 and subsequent fines from the Information Commissioner's Office.

Once a PIA has been completed, the document must be forwarded to the IGSG for approval and sign off.

14 Business continuity plans

Business Continuity Management is a method used to identify potential impacts that may threaten the operations of the CCG's business/premises. The fundamental element of business continuity is to ensure that whatever impacts the CCG, the organisation continues to operate. Business continuity plans will help shape organisational resilience to 'threats', plan counteractions and minimise interruptions to the CCG's activities from the effects of major failures or disruption to its Information Assets (e.g. data, data processing facilities and communications).

Each team should have Business Continuity Plans in place and it is the responsibility of members of staff to be aware of the location of plans, and what procedures to follow in the event of potential 'threats' to the operation of the CCG.

For further information regarding Business Continuity Plans, please contact your line manager or the most senior member of staff in your department.

15 Information sharing

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The CCG needs to ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

Staff sharing personal information with other agencies should be aware of the requirement to have an Information Sharing Agreement (ISA) 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.

Information sharing agreements document:

- The purpose for the information to be shared/purpose of the protocol
- What information will be shared

- Who the information will be shared with
- Senior Management/Executive endorsement of information sharing protocol
- Structures of sharing information
- Legislation and regulations which are required to be adhered to under the Data Protection Act 1998.

For further advice and guidance on Information Sharing Agreements, please contact the IG CO

Information sharing procedure

- Sharing of information can only be authorised by either the CCG's IGSG, Caldicott Guardian and IGSG
- It is the responsibility of each staff member to manage the risks to security of information when it is shared.

To prevent the risk of information security incidents or breaches, **all staff must:**

- Consider what information is being requested and ensure the proposed use is valid.
- Only use confidential information when absolutely necessary. Assess whether the stated purpose could be accessed via alternative route. If it can, the information must not be shared.
- Use minimum information required, i.e. only share information which is necessary to the purpose.
- Limit access to the information, it should only be accessed by a limited number of authorised personnel to carry out task.
- Ensure, if information is transferred, that security measures are in place.
- Consider all legal requirements under the **Data Protection Act 1998**.

16 Smartcards

Smartcards are required to use and access IT systems essential to healthcare provision. Primary Care Contractors need to use Smartcards in order to gain access to patient information .i.e. those who provide the Choose and Book service and the Electronic Prescription Service.

Individuals are granted access to a Smartcard by the organisation's Registration Authority lead. It is up to the Registration Authority Team to verify the identity of all healthcare staff who need to have access to patient identifiable or sensitive data. Individuals are granted access based on their work and their level of involvement in patient care. The use of Smartcards leaves an audit trail.

Staff should be aware that disciplinary action may be taken if Smartcards are shared or lost.

Line manager responsibilities

- To identify all roles within their area of responsibility which require access to the system and ensure that all employees, including temporary/agency/bank and locum employees, are provided with appropriate access.
- To ensure for all roles that involve access to the system that job descriptions and any recruitment materials make reference to the need to be registered and the role's responsibilities in relation to using the system.
- To ensure that all new starters within their area of responsibility, including agency/temporary employees, receive training in order to be able to access the system.

- To ensure that all employees are aware of Information Governance policies, associated documentation and their responsibilities in relation to use of and access to the system.
- To immediately inform the CSU Information Governance Team, of any leavers, starters and staff changes.

Staff smartcard code of practice

- Use your Smartcard responsibly and in line with your access rights.
- Inform the South East CSU Registration Authority team or their IG CO immediately should your Smartcard be lost, stolen or misplaced.
- Ensure that you report any misuse of the Smartcards
- Ensure that you keep your Smartcard and log-in details confidential. In particular you must not leave your PC logged in and you must not share or provide access to your Smartcards or passwords.
- Ensure that you accurately complete the necessary paperwork, provides suitable identification and attends any appropriate appointments in order to register on the system or have your Smartcard updated/re-issued.
- All members of staff using Smartcards should follow the organisation's suite of Information Governance policies and procedures; adhere to the Data Protection and Caldicott Principles, and the Confidentiality Code of Practice and the Care Records Guarantee.

17 Key Information Governance contacts

Senior Information Risk Owner (SIRO)	Mathew Knight
Caldicott Guardian:	Dr Andy Sharpe

Information Governance Leads

Governing Body Secretary	Justin Dix	Justin.Dix@surreydownsccg.nhs.uk
South East CSU Principal Associate - Information Governance SME (IG SME)	Milton Shoriwa	milton.shoriwa@nhs.net
South East CSU – Senior Associate Information Governance Compliance Officer(IG CO)	Abdel Montasir	abdel.montasir@nhs.net

18 Confirm you have read and understand this IG Staff Handbook

Please ensure you

1. Sign the accompanying slip confirming you have read and understood the information provided
2. Return to the Human Resource team or the IG CO.

Should you have any questions or queries regarding information governance, please do not hesitate to contact any of the IG Leads above.

NHS
Surrey Downs
Clinical Commissioning Group

Information Governance staff handbook confirmation slip

I confirm that:

I have received my copy of the Information Governance Staff Handbook and I understand my responsibilities.

Name
Signature
Job Title
Workplace

Please return to:

Surrey Downs Clinical Commissioning Group
Human Resource Team or the IG Compliance Officer,
Surrey Downs Clinical Commissioning Group,
Cedar Court,
Guildford Road,
Leatherhead, Surrey,
KT22 9AE

By Email: hr@surreydownsccg.nhs.uk