Buckinghamshire

Clinical Commissioning Group

Information Governance Staff Handbook

Version 2.4 – January 2021

Document type:	Guidance Document
Document title:	**Information Governance Staff Handbook**
Document date:	January 2021
Author:	Information Governance SCW CSU
Approved by:	**Information Governance Steering Group (approval), CCG Audit Committee (ratification)**
Approval date:	January 2021
Version:	V2.4
Review date:	January 2022

Amendments Summary:

Amend No	Page(s)	Subject	Action Date
1	All	Extensive reformatting, additional wording, including changes under the Data Protection Legislation throughout document	04/04/18

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2.0	03.04.18	Matt Wall, Angela Sumner & GDPR working group		Updates incorporating changes to Data Protection Legislation
2.1	11.10.18	BCCG IGSG		CCG IGSG to review the policy in light of new legislative requirements. No changes.
2.2	04.12.19	BCCG IGSG		Annual Review only, no changes expect to insert link to 2020 version on CCG G drive
2.3	January 2020	Russell Carpenter		Insertion of section on paper light/paperless office principles
2.4	January 2021	Russell Carpenter		1. Minor edits including addition of narrative following incident learning - addition to definitions for data controller, data processor, addition of categories for legal basis under common law duty of confidentiality (consent, legal duty, public interest etc.) and description of legal bases applied under GDPR when a legal basis under common law duty of confidentiality has already been established.

				2. Project management: *Buckinghamshire CCG has decided that a DPIA process will be embedded into its Project Management Verto system and a completion of DPIA screening question is now mandatory at the 'mandate stage' of the project itself* – text removed as already referred to elsewhere and Verto system now no longer in use. 3. Confirmation slip re-edited as text for email confirmation of receipt of handbook. When the handbook is circulated to staff, all are asked to that: *I have received my copy of the Information Governance Staff Handbook and I understand my responsibilities.* Reply emails shall include electronic signature. The reply returned to the CCG IG Lead, Data Protection Officer (or other staff member whom circulates it) shall also be date and time stamped. 4. G Drive location for other policies updated to 2021. Note added to folder: *Apart from the Information Governance handbook reviewed and updated in January 2021, all other policies and procedures contained within the equivalent folder for 2020 remain valid until such a time as they have been reviewed and updated.*

Contents

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 data and special categories of personal data, as defined in Data Protection Legislation is:

- Processed Lawfully, Fairly and Transparently
- Collected for specified, explicit and legitimate purposes
- Adequate, Relevant and not excessive
- Accurate and kept up to data
- Kept for no longer that is necessary and
- Processed in a secure manner

NHS organisations hold large amounts of personal, commercially confidential and special categories of personal data, and all staff should be able to provide assurance that the Information Governance standards are incorporated within their working practices. All organisations must be able to evidence their compliance with Data Protection Legislation in order to fulfil the principle of Accountability.

Personal and special categories of personal data can be contained within a variety of documents. For example:

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

For clarity, the use of the terms data and information have a precise meaning and the words are not interchangeable. For the purposes of this handbook

Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'

Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'

Legislation and Regulations

Members of staff should be aware of the Data Protection Legislation that govern how organisations must safeguard information, what processes should be in place to use, secure and transfer information and also how patients and members of public can exercise their rights under that legislation. This area is complex but can be viewed as follows.

Data Protection Legislation can be used as a generic term which encompasses the following:

- the Data Protection Act 2018 (DPA 2018)
- the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679),
- the Law Enforcement Directive (LED) (Directive (EU) 2016/680)
- regulations made under the DPA 2018
- any applicable national Laws implementing them as amended from time to time

- all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

In addition, organisations must take account of the following as part of their information governance and management practices:

- Freedom of Information Act 2000
- Environmental Information Regulations
- INSPIRE Regulations
- Health and Social Care Act 2012
- Access to Health Records Act 1990
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988

The organisation must also have regard for the following standards and Codes of Practice:

- International information security standard: ISO/IEC 27002: 2005
- Caldicott Principles
- Data Security and Protection Toolkit
- Data and cyber security: protecting information and data in health and care
- Data Sharing - Data Protection Code of Practice - ICO
- Codes of practice for handling information in health and care
    - Records Management Code of Practice for Health and Social Care
    - Code of practice on confidential information
    - HSCIC Guide to Confidentiality
    - Confidentiality
    - Information security management NHS code of practice
    - NHS Information Governance - Guidance on Legal and Professional Obligations
- Confidentiality Supplementary Guidance - Public interest disclosures
- CCTV
- Privacy notices, transparency and control
- ICO guidance - Anonymisation
- Personal Information Online Code of Practice

The Buckinghamshire Clinical Commissioning Group (BCCG) has produced a suite of policies, processes and procedures, which can be found on the G Drive.

G:\AVCCG CCCG SCWCSU\Policies & Procedures\Information Governance\IG policies and handbook 2021

Adherence to Information Governance principles ensures compliance with the law, best practice and embeds processes that help staff manage information appropriately. It must also be noted that embedding information governance processes enables patient's, service users and the general public to have greater trust in the CCG and enables effective working across partner organisations.

Information Governance Structure

Accountable Officer

The CCG Accountable Officer has overall responsibility for Information Governance 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 (SIRO)

The Senior Information Risk Owner for the CCG is an executive board member with allocated lead responsibility for the organisation's information risks and provides the focus for management of information risk at Board level. The SIRO must provide the Accountable Officer with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted by the organisation. The SCW Information Governance Manager will support the SIRO in fulfilling this role.

Caldicott Guardian

The Caldicott Guardian is the person within the CCG with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the CCG Board and relevant committees on confidentiality issues. The SCW Information Governance Manager will support the Caldicott Guardian in fulfilling this role.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been identified within the CCG that has the responsibilities as set out in the GDPR guidance, such as monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and ICO

SCW Information Governance Manager

The SCW Information Governance (IG) Manager supports the CCG DPO in ensuring that the Information Governance programme is implemented throughout the CCG. The IG Manager is also responsible for co-ordinating a number of activities that contribute to the completion and annual submission of the Data Security and Protection Toolkit for the CCG. The IG Manager will support the CCG's SIRO, Caldicott Guardian and DPO in investigating Serious Incidents Requiring Investigation (SIRIs), offer advice and ensure the organisation complies with legislation, policies and protocols as per the SLA.

Information Asset Owners (IAO)

The SIRO is supported by Information Asset Owners (IAOs). The role of the 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 IG Manager will support the IAOs in fulfilling their role.

Data Custodians (DC's)/Information Asset Administrators (IAA's)

This important role is required to support the IAO's and SIRO who will work with the Information Governance Team to ensure staff apply the Data Protection Legislation and Caldicott Principles within working practices. The IG Manager will provide local face to face IG training if required and will monitor staff compliance by way of the consult OD portal and link to the e-LfH platform.

https://www.consultod.co.uk/login/index.php

https://nhsdigital.e-lfh.org.uk/

The username is the user's email address, with a prompt to reset the password.

Caldicott Principles and Data Protection Legislation Principles

The Caldicott Principles

The National Caldicott Guardian has previously made recommendations aimed at improving the way the NHS uses and protects confidential information; these have been updated in subsequent reviews. 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 personal confidential data unless absolutely necessary – Can the task be carried out without identifiable information?

Principle 3: Use the minimum necessary personal confidential data – Can the task be carried out with less information?

Principle 4: Access to personal confidential data should be restricted to required/relevant personnel.

Principle 5: Everyone with access to personal confidential data 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

Caldicott 1 Caldicott 2 Caldicott 3

The Data Protection Legislation and Principles

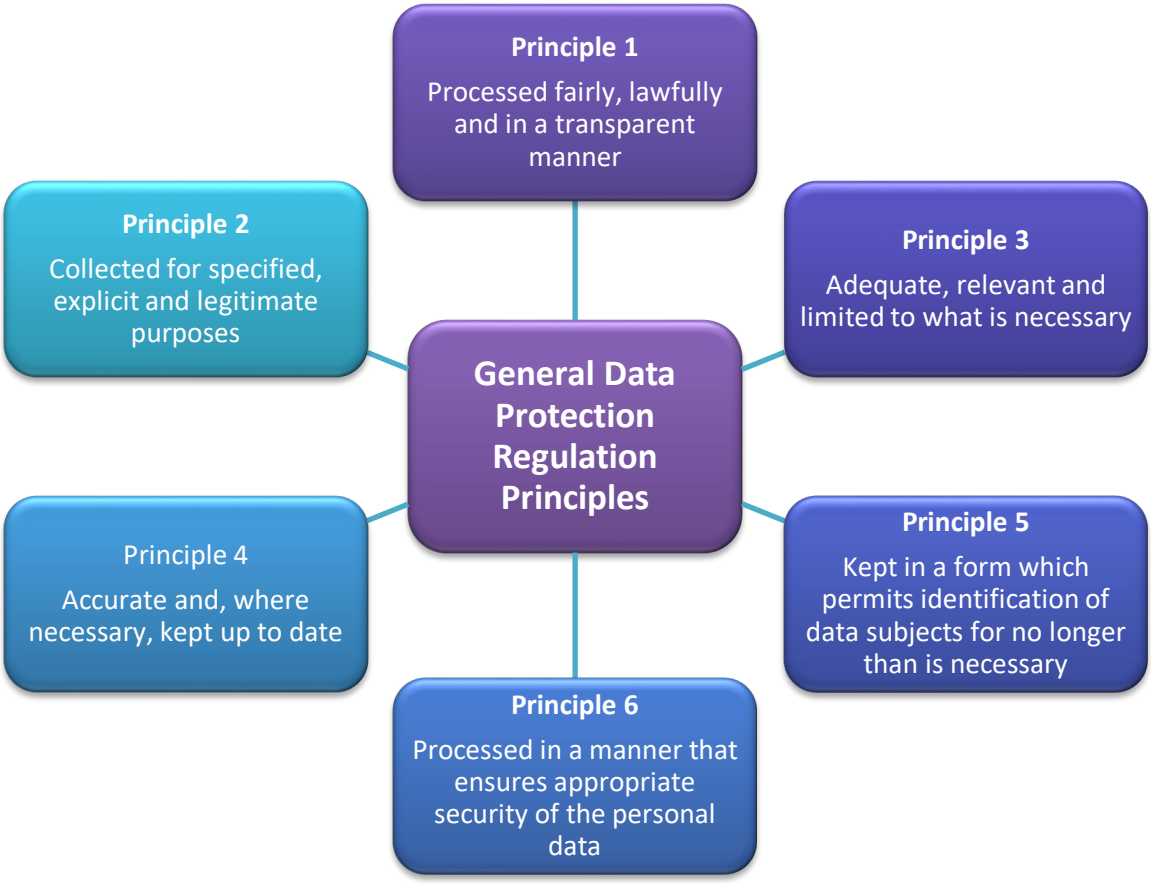
All organisations in the UK must comply with the Data Protection Legislation which has the meaning as described in the Data Protection Act 2018 part 1, 3 (9). The Data protection Legislation is enforced

in the UK by the Information Commissioner's Office (ICO) who has the power to impose penalty notices on organisations based on two tiers the "higher maximum amount" up to €20m or 4% of total annual turnover, whichever is the greatest or the "standard maximum amount" up to €10m or 2% of total annual turnover, whichever is the greatest.

Under the legislation it is not just data breaches which can attract a fine, non-compliance with the Regulations can also be subject to fines which is why under the additional new principle of 'Accountability' organisations must be able to provide evidence of compliance.

Accountability: GDPR Article 5 (2) "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The following are the six General Data Protection Regulation principles (Article 5) that must be followed when handling personal and special categories of personal data. These principles should be considered when handling both corporate and clinical records.



In addition, the Data Protection Legislation requires the 'controller', (meaning as defined in chapter 2 (6) of the Data Protection Act 2018), to demonstrate, compliance with these principles

These Data Protection Legislation and Caldicott principles translate into **key rules 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 and Special categories of personal data may be disclosed
- Individuals have legislated rights including the right to information, the right of access, the right to rectification and erasure, the right to restrict processing, the right to data portability and the right to object to various types of processing of their data
- Identifiable information should be anonymised or pseudonymised wherever and whenever possible
- The disclosure or sharing of personal data is permissible where there is a legal obligation to do so, an exemption can be applied or where the individual has given explicit consent
- Sharing of personal data between organisations must take place with appropriate authority, safeguards and agreements in place
- 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
- An organisation must be able to provide evidence to show compliance with the Data Protection Legislation requirements and principles

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.

The **common law duty of confidentiality** is usually relied upon as a legal basis for sharing or processing health records data. This may comprise:

- **Consent** of the data subject (Explicit, Informed or Implied)
- **Reasonable expectation** of the Data Subject – that their data shall be shared for direct care purposes without specifically informing them, e.g. sending a referral from GP practice to hospital.
- **Legal duty or power*** – e.g. a section 251 agreement (a power from the NHS Act 2006) which allows the Secretary of State to suspend confidentiality requirements (e.g. validating invoices), or relevant safeguarding acts.
- **Public interest** (i.e. court order) – which is rarely proven as a legal basis where health records are shared or processed
- Consent under GDPR for sharing or processing health records data is irrelevant

  * These are different – an act or regulation may set out a power that allows an individual or organisation to do something, whereas a duty is something an organisation or individual must do to comply with that act or regulation (e.g. sharing PID related to safeguarding in the event that gaining consent would endanger the lives of the child)

What is Personal Data?

As described in part 1, subsection 3 of the Data Protection act 2018

(2) "Personal data" means any information relating to an identified or identifiable living individual
(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) an identifier such as a name, an identification number, location data or an online identifier, or
(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

What are "Special Categories of Personal Data"?

As described in article 9 of the GDPR, special categories of personal data are Personal Data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) the processing of genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health or
h) data concerning a natural person's sex life or sexual orientation

Under the **Data Protection Legislation** staff can only process or have access to personal data if:

- An appropriate condition for processing (GDPR Article 6 and Article 9) and a supporting lawful basis has been identified and documented in a statutorily required (DPIA) or,
- Explicit consent has been obtained from the individual or,
- The data has been anonymised or pseudonymised in line with Dara Protection legislation requirements; or
- The data is in respect of safety, safeguarding or in the public interest. Any decision taken to share Personal or Special Categories of Personal Data that is by its nature, owed a duty of confidentiality as a result of the above should be discussed with the DPO, documented in the DPIA and agreed by the Caldicott Guardian

Staff should check with the DPO, supported by the SCW IG Manager, if they have any queries on whether to access or process Personal or Special Categories of Personal Data.

Legal bases applied under GDPR

Staff should not that where a legal basis is identified under common law duty of confidentiality, then a legal basis of consent under GDPR will be irrelevant. This explains why other legal bases under **GDPR** are cited, usually:

- Processing personal data is Article 6 paragraph 1 (e) "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*".
- **BUT** it is mistaken to think that it is the "*public interest*" which is the legal basis. Rather it the "*official authority*" which is the legal basis to process health records data under GDPR.
- This "*official authority*" is where a clear legal basis under UK law can be pointed to such as NHS Act 2006 or Health and Social Care Act 2012.

- It is important to note that an individual power or duty does **NOT** have to be identified within the law in order to prove the legal basis exists.
- processing special category of personal data (health) is Article 9, paragraph 2 (h): "*processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care systems and services on the basis of Union or Member State Law or pursuant to contract with a health professional*"
- **BUT** this can be applied only if there is already a legal basis for sharing or processing under article 6.

Personal Confidential Data

Although an organisation within the NHS may have identified a lawful basis to process data, including special categories of personal data, this does not necessarily mean that the information can be used or shared in a way that identifies the individual if that information has been obtained where a 'duty of confidence' is owed.

In practical terms this means that if a GP wanted to share information with another care organisation that is providing care to that Patient e.g. an acute or community hospital, as long as the GP believes that the Patient would raise no objection and that it would be within their reasonable expectations for them to do this then this sharing is permitted and encouraged within the law. If however the GP wishes to share information that identifies a Patient and was obtained confidentially with someone else e.g. a charity, an advocate or the CCG, unless there are reasons why this must happen due to statutory obligations or it is in the public interest to do so, the Patient must be given the opportunity to consent to this happening.

It may be easier to consider the following

What information?	Category of data	How was it obtained?	Is it confidential?
Name and address and postcode	Personal Data	Electoral register	No
Full Postcode, recent hospital admissions, age, marital status	Personal Data and Special category of personal data	Performance report	Yes – measures to reduce the risk of identifying the person should be taken by reducing the postcode search criteria
Member of local church	Special Category of Personal Data	Facebook members group post	No – made public by the individual
Religious belief limiting health care	Special Category of Personal Data	Patient to GP consultation	Yes – GP would only share if Patient would expect this for their care
Date of surgery on knee	Special Category of Personal Data	Individual posted photo of themselves in hospital	No – made public by the individual
Date of surgery on knee	Special Category of Personal Data	GP included in request for further funding for additional operation	Yes – GP would only share if Patient would expect this for their care
Sexual orientation	Special Category of Personal Data	Identifies own orientation on social	No – made public by the individual

		media or other public forum	
Sexual orientation	Special Category of Personal Data	Consultant includes information on gender reassignment status within hospital record	Yes – highly confidential and Consultant would only share if Patient would expect this for their care or has given explicit consent

Commercially confidential data

This describes information that is owed a duty of confidentiality concerning the organisation and its business. This includes trade secrets, parts of the procurement and contracting process and also information it may hold that has been given to it by a third party. Further guidance on what constitutes commercially confidential data can be found here ICO guidance.

Information Sharing and Data Sharing Agreements

It is important to ensure that there is a balance between sharing information with others 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 only takes place within legal limits.

Information Sharing (within the CCG)

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

- Only use PCD when absolutely necessary – assess whether the stated purpose could be achieved via alternative method. If it can, the information must not be shared with colleagues;
- Consider what information is being requested – ensure the proposed use is valid;
- Use minimum information required - only share information which is necessary to the purpose;
- If information is transferred ensure security measures are in place (use NHS net to NHS net);
- Consider all legal requirements under the Data Protection Legislation;
- Limit access to the information – information should only be accessed by personnel authorised to carry out the task;
- It is the responsibility of each staff member to manage the risks to security of information when it is shared; and
- Any decision taken to share personal confidential data as a result of the above must be documented and agreed by the SIRO and Caldicott Guardian.

Information Sharing (outside the CCG)

In addition to the above, staff that have been asked to share information *outside* of the organisation must also check that there is an agreed Data/Information Sharing Agreement in place. A Data Sharing Agreement should be put in place where a number of organisations wish to share information or data for a common purpose. An example of this could be a group of CCG's who want to share information across all of their geographical areas to look into the use of an acute hospital (see also DPIAs above). The agreement must include the lawful basis for sharing the information and be clear on the responsibilities of each organisation in relation to that information.

Advice should always be sought from the CCG's DPO and such agreements **must** be approved by the CCG's SIRO or Caldicott Guardian **before** any information can be shared.

Data Sharing Agreements document must include:

- The purpose for the information to be shared/purpose of the agreement
- What information will be shared
- Who the information will be shared with
- Senior Management/Executive endorsement of data sharing agreement
- Structures of sharing information
- The legal basis in which the information is being shared in adherence to the Data Protection Legislation

For further advice and guidance on DSA's, please contact the SCW IG Manager for the CCG who may be able to provide a standardised template for you to adapt to the particular situation where information is being shared.

Data Processing Agreements

A Data Processing Agreement (DPA) is needed whenever a controller uses a processor (e.g. SCW who processes personal data on behalf of the CCG). Similarly, if a processor employs another processor (sub-processor) it needs to have a written agreement in place.

Agreements between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of agreements by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

Agreements must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the controller.

Agreements must also include a number of standard items and guidance is available from the SCW IG Manager. It is important to remember that every processing activity may be different and whilst there will be common agreements in place e.g. between the CCG and SCW, each must be assessed through the completion of a DPIA to ensure that no changes are needed to the standard template.

If a processor fails to meet any of the obligations in the agreement, or acts outside or against the instructions of the controller (the CCG), then it may be liable to pay damages in legal proceedings, or be subject to fines or other penalties or corrective measures.

If a sub-processor is used then it will, as the original processor, remain directly liable to the controller for the performance of their obligations.

New or Existing Programmes and Projects

Data Protection Impact Assessments

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, staff must consider IG implications when starting new projects and programmes. The Data Protection Impact Assessment (DPIA) is the tool used to help identify Data Protection implications and this process, and time required for it to take place,

should be built into the project plan. DPIAs should be undertaken at the start of a programme and project - i.e. the 'project initiation stage' aka mandate stage.

Using a DPIA at the project initiation stage will help the CCG to:

- identify and address Information Governance issues at an early stage, reducing any associated costs and damage to reputation which might occur if processes are not compliant with the law
- avoid delays to projects caused by implementing any late changes that are required in order to be IG compliant
- identify where information sharing agreements need to be put in place
- ensure the CCG is aware of, and can effectively monitor, the data it is using

It will also minimise the potential of failing to comply with the Data Protection legislation and therefore minimises the potential for the CCG being issued with a notice and fine from the Information Commissioner's Office.

Under the Data Protection Legislation the completion of a DPIA is a statutory requirement where the type of processing is likely to result in a high risk to the rights and freedoms of the public and in particular in the cases of:

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing
- Processing on a large scale of special categories of data referred to in GDPR article 9(1), or article 10; or
- Systematic monitoring of a publicly accessible area on a large scale.

A template, guidance documents and other checklists to help with a DPIA are available. In line with Data Protection Legislation, the organisations DPO must be included and allowed to advise on the proposed project/processing as part of the DPIA process. When requested, the SCW Information Governance Team can support the DPO to review and risk-assess DPIAs to help establish the Information Governance implications. The CCGs SIRO, taking into account the comments and recommendations of the DPO, must give final approval of the DPIA before the project should proceed.

Individual rights under the GDPR

The GDPR confers rights on individuals that can be exercised in certain circumstances. In brief, an individual has

a) The right to be informed (articles 12 to 14)
b) The right of access (article 15)
c) The right to rectification (article 16 and 19)
d) The right to erasure (article 17 and 19)
e) The right to restrict processing (article 18 and 19)
f) The right to data portability (article 20)
g) The right to object (article 21)
h) The right not to be subject to automated decision making and profiling (article 22)

<u>The right to be informed</u>

This means that the Controller should provide information and communications relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain

language, taking into account the age of the audience (e.g. Children). This is usually done through a Fair Processing Notification (FPN) which will be on an organisations webpages, on posters or leaflets or using a mixture of all of these methods. There are certain criteria that need to be met and specific information included. Ask the SCW IG Manager for more information or go to ICO guidance - right to be informed

Paul Antony |Information Governance Manager

NHS South, Central and West Commissioning Support Unit, Jubilee House, 5510 John Smith Dr, Oxford, Oxfordshire OX4 2LH. | Mobile: 07786 700021 | Email: paul.antony@nhs.net | SCWCSU.IGEnquiries@nhs.net

Requests under the right of access (Subject Access Requests)

Under the Data Protection legislation , 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 categories of data held, the purposes for which it is processed and to whom it may be disclosed
- A copy of any information held
- To be informed as to the source of the data held
- Where automated decision-making has taken place, data subjects must be informed about the logic involved and envisaged consequences of such processing for the data subject

Support will be given to the Data Custodians to ensure all requests are responded to in line with the **one** calendar month legislative timescale.

Copies of records requested must be made available free of charge unless the request is manifestly unfounded or excessive, particularly if it is repetitive. Advice should be sought from the Information Governance Team if a charge is being considered so that the reasons why a charge has been applied can be fully documented.

Staff should notify their Data Custodian immediately on receipt of a right of access request. The CCG right of access request guidance should be used as the agreed procedures and each request should receive prompt attention.

As a staff member, your personal information can only be obtained through the right of access request process, refer to the individual rights policy for further information. If you access your personal information through systems used within the CCG, other than that which are permitted such as ESR, disciplinary action will be taken.

The right to rectification

An individual can exercise the right to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. You have one calendar month to respond to a request. In certain circumstances you can refuse a request for rectification.

Support will be given to the Data Custodians to ensure all requests are responded to in line with the **one** calendar month legislative timescale. Staff should notify their Data Custodian immediately on receipt of a request. The CCG right to rectification guidance should be used as the agreed procedures and each request should receive prompt attention.

The right to erasure (article 17 and 19)

An individual has the right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. You have one month to respond to a request. The right is not absolute and only applies in certain circumstances.

Support will be given to the Data Custodians to ensure all requests are responded to in line with the **one** calendar month legislative timescale. Staff should notify their Data Custodian immediately on receipt of a request. The CCG right to erasure guidance should be used as the agreed procedures and each request should receive prompt attention.

The right to restrict processing (article 18 and 19)

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, you are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. You have one calendar month to respond to a request. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Support will be given to the Data Custodians to ensure all requests are responded to in line with the **one** calendar month legislative timescale. Staff should notify their Data Custodian immediately on receipt of a request. The CCG right to restrict processing guidance should be used as the agreed procedures and each request should receive prompt attention.

The right to data portability (article 20)

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. Some organisations in the UK already offer data portability through the midata and similar initiatives which allow individuals to view access and use their personal consumption and transaction data in a way that is portable and safe.

Support will be given to the Data Custodians to ensure all requests are responded to in line with the **one** calendar month legislative timescale. Staff should notify their Data Custodian immediately on receipt of a request. The CCG right to data portability guidance should be used as the agreed procedures and each request should receive prompt attention.

The right to object (article 21)

Individuals can object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

You must stop processing the personal data unless: you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims. You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

Support will be given to the Data Custodians to ensure all requests are responded to and staff should notify their Data Custodian immediately on receipt of a request. The CCG right to object guidance should be used as the agreed procedures and each request should receive prompt attention.

The right not to be subject to automated decision making and profiling (article 22)

The GDPR has provisions on: automated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them. You can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent

You must identify whether any of your processing falls under Article 22 and, if so, make sure that you:

- ✓ give individuals information about the processing;
- ✓ introduce simple ways for them to request human intervention or challenge a decision;
- ✓ carry out regular checks to make sure that your systems are working as intended

For further guidance on this please see the CCG Individual Rights Policy and guidance document.

Some of the ways you can help keep information secure and confidential:

Know the CCG's organisational arrangements including key IG job roles

Make sure you know the name of the following as you may need to consult with them:

- The CCG SIRO
- The CCG Caldicott Guardian
- The SCW IG Manager
- The CCG Data Protection Officer
- Your team's Information Asset Owner
- Your team's Data Custodian

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
- 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 (Ctrl+Alt+Delte or 'Windows Key'+L)

Ensuring authorised access only

- Access to records must be on a "need to know" basis only

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 in accordance with the Records Management Code of Practice and the Data Protection Legislation. The appropriate retention schedule must be documented on the appropriate Data Flow Map for the area.
- Ensure any personal or special categories of personal data are confidentially destroyed in accordance with the CCG Information Security policy. (Note that ordinary waste bins and 'recycling' bins are not to be used for papers showing personal, commercially confidential or special categories of personal data).
- Dispose of redundant equipment, especially disk or tape copies of personal, commercially confidential or special categories of personal data, in the proper manner through the CCG's ICT provider (SCW).

Off-site working

- Do not take personal, commercially confidential or special categories of personal data out of the office and especially off-site unless authorised
- If you are authorised to take information off-site, always make sure that a list of the records/information 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 sight in the boot of the car and removed to a place of safety on arrival at your destination

Requests for information

If you receive a request for information about the organisation refer to the FOI section below. For requests relating to a patient, staff member, etc. and where it is not usually part of your job to respond refer to the Subject Access Rights Request section

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

Disclosures

You may, as part of your job, need to disclose patient/personal 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
- Ensure that personal, confidential and special categories of personal data are only disclosed to a non–NHS organisation in accordance with the law, after a DPIA and any relevant and necessary agreements are in place; if in doubt, refer to the SCW IG Manager

Patient contacts and patient details

- Do not leave messages that contain personal, commercially confidential or special categories of personal data 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, commercially confidential or special categories of personal data should not be visible to the public
- Any notes containing personal, commercially confidential or special categories of personal data written whilst taking a phone call or other message should be destroyed securely

Transferring personal, commercially confidential or special categories of personal data

The ICO has imposed monetary penalties on organisations who have failed to comply with the Data Protection Legislation due to insecure transfers of information via fax, post and emails. 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 information.

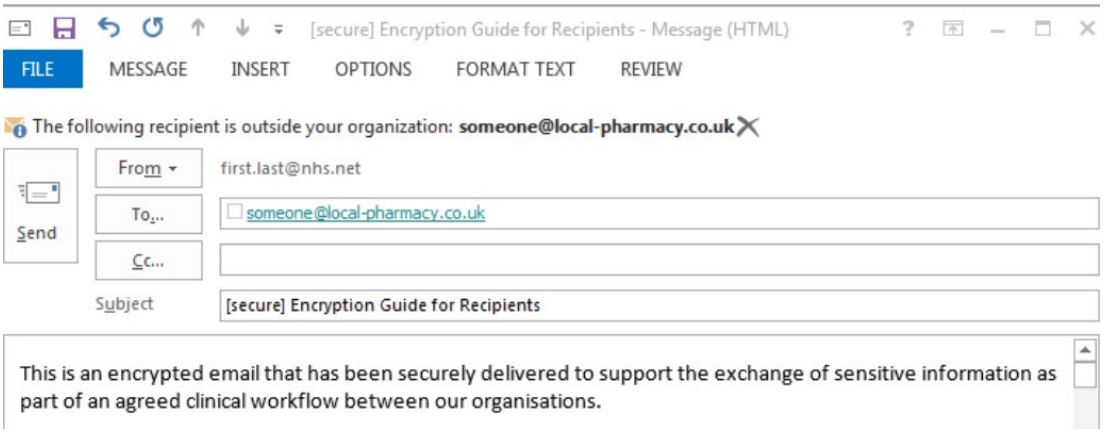
NHSmail Process

It is policy that emails containing any confidential or commercially sensitive information should be sent using an NHS.net account. Therefore, if you're emailing from your @nhs.net account to another @nhs.net account, then you can be confident that the content of your message is encrypted and secure.

Guidance for sending emails to non-secure domains.

There have been changes in the way that NHSmail sends emails with confidential data to other email systems. When sending emails with confidential data outside of NHSmail you must use [secure] in the subject line of your email (the word secure must be in square brackets as in screenshot below), [secure] is not case sensitive. The Encryption Guide for NHSmail must be followed to ensure you understand all guidance and instructions on using this feature.

Example screen shot below:



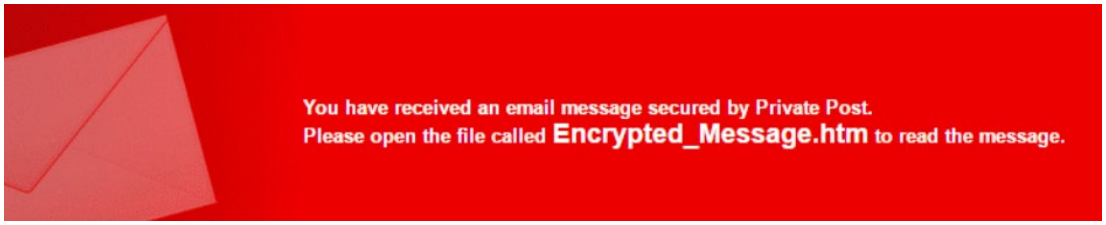
Guidance for Accessing Encrypted Emails

An encrypted email sent from an NHSmail address (ending @nhs.net) will contain a link to access the encrypted message.

PRIVATE AND CONFIDENTIAL

You have received an email message secured by Private Post. Please open the file called Encrypted_Message.htm to read the message.

(example of an encrypted NHSmail email message)



(example of an encrypted NHSmail in Gmail)

The NHSmail Accessing Encrypted Emails Guide must be followed to ensure the recipient follows the registration process in order that they are set up with an account with the NHSmail encryption provider. The Guide also provides advice on replying and forwarding encrypted emails.

The NHSmail portal (https://portal.nhs.net), NHSmail Support Site will provide you with information and guidance on sending and receiving emails outside the NHSmail service – please refer to the Sharing Sensitive Information Guidance.

As a user of the NHSmail platform you must operate in accordance to the published guidance, policies and procedures to ensure you are using NHSmail effectively, appropriately and safely. Please refer to the materials below to ensure you are adhering to NHSmail guidance:

- NHSmail Acceptable Use Policy (AUP)
- Information Management Polices
- Sharing Sensitive Information Guidance
    - Encryption Guide for NHSmail
    - Accessing Encrypted Emails Guide

- Encryption Guide for Senders

Do not put personal confidential or special categories of personal data in the subject header when sending an email.

Please seek advice from the SCW Information Governance Manager if required.

E-mail guidance:

- Check what you are 'forwarding' or sending, when using the 'reply all' option in case the information is not intended for further sharing
- Ensure that any attachments do not include information that should not be shared such as hidden tabs of Patient names or identifiers
- Make sure you select the correct recipient from the address book
- Remember that any email you send that contains information about an identifiable individual could be disclosed under the right of Subject Access (see below)
- Good management of emails and folders is essential
- Sending CCG information to private or personal email accounts should be avoided
- Don't overuse the 'cc' option, only send to those who need the information and not 'just in case'. Think very carefully about using the 'Bcc' option, it is appropriate for protecting the anonymity of recipients but not in every situation.
- Confidential messages must not be forwarded without the consent of the sender.
- Setting up an automatic forward to a private email address from a NHSmail account is strictly prohibited
  Unsolicited emails must not be sent.
- Emails must not be forged or attempted to be forged.
- Do not send email messages using another person's email account for whatever reason – if you need to access someone else's email, for example during periods of annual leave – then this can be set up in Outlook. IT Helpdesk can help you with this.
- Do not breach copyright or licensing laws when composing or forwarding emails and email attachments.
- Using any other email address other than your NHS.Net account to send corporate information or personal identifiable information/data is prohibited - see "Safe Haven Policy and Procedure"
- Personal use is permitted however this should be kept to a minimum and should not interfere with work.
- Personal emails must adhere to the guidelines in this policy.
- Personal emails must be deleted when read to prevent undue burden on the email system.
- The forwarding of chain emails, junk mail, jokes and executables is forbidden.
- Users must not send emails using any other users login details or accounts.
- The CCG will ensure that all users are properly trained in using the email system.
- It is the responsibility of all managers and staff to ensure that any training needs are identified, so that the CCG can arrange suitable training.
- The CCG will ensure that all emails, incoming and outgoing, are monitored for viruses.
- The CCG will monitor and log all email traffic – however the content of emails will not be logged.
- The CCG will not routinely monitor emails for content; however it reserves the right to retain message content as required to meet both legal and statutory obligations.

- All emails remain the property of the CCG and represent part of the organisations corporate history. It is for this reason that private email accounts should not be used to conduct CCG official business.
- The CCG reserves the right of audit in respect of private emails downloaded onto CCG equipment. The personal use of private emails is permitted if it does not interfere with the service delivery requirements of the CCG.
- Emails received in error – you must notify the sender and ensure that the email and any associated attachments are deleted.
- Emails sent in error – you should immediately notify the recipient(s) to disregard the email and delete the email and any attachments. Inform your line manager and advise the Information Governance Manager. Follow Incident Management procedures as necessary.

It is strictly prohibited to send or forward emails containing attachments, remarks or depictions that could be considered;

- libellous
- defamatory
- offensive
- harassing
- racist
- obscene
- pornographic

If you receive an email of this nature, you must promptly notify your manager or supervisor.

Safe Haven Processes

Fax

Fax machines must only be used to transfer personal, commercially confidential or special categories of personal data 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 information containing personal, commercially confidential or special categories of personal data 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 information that includes personal, commercially confidential or special categories of personal data 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 confidential ensure someone is at the receiving end waiting for it
- Ensure only authorised staff handle confidential information
- If you receive faxes that contain confidential information store them in a secure environment
- Fax machines should be turned off out of hours

Postal service

It is recommended that staff members follow these guidelines:

Some examples of documents that may need added protection when sending mail are:

- ✓ Birth Certificates
- ✓ Driving Licences
- ✓ Marriage Certificates
- ✓ Passports
- ✓ Bank statements and other financial information

- Send information that includes personal, commercially confidential or special categories of personal data by 'Royal Mail Signed For' or 'Royal Mail Special Delivery Guaranteed' or 'private courier' but always assess the risk first to determine the most appropriate delivery method. For postage rates and assistance with assessing which method is the most appropriate for the documents see http://www.postoffice.co.uk/mail
- Double envelope the documents for added security
- Ensure that the address is written clearly and in indelible ink and ensure post is sent to a named person or department
- Clearly mark the top envelope with 'private and confidential for the addressee only'
- Include a return to sender address on the back of the envelope
- Confirm receipt with the intended recipient as early as possible

The Information Commissioner has issued further guidance regarding the potential for Identity Theft which can be found at ICO guidance on Identity Theft.

Paper documents

All records containing personal and confidential data must be stored face down in public areas and not left unsupervised at any time.

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

Make a log of what notes have left the department (e.g. home visits etc) and record when they are returned (where appropriate).

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

Computers

Do not share logons and passwords with anyone

Computer screens must not be left on view so members of the general public or staff who do not have a justified need to view the information can see personal data. “Press Control Alt Delete Every Time You Leave Your Seat”.

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

Personal and confidential data should be held on the organisation’s network servers, not stored on local hard drives or desk top removable media. Where removable media are used such as laptops or memory-USB sticks, these must be encrypted.

Personal and confidential data must not be saved or copied into any PC or media that is ‘outside the NHS’.

Telephone Calls

Do not make telephone calls discussing personal or confidential data where you can be overheard (e.g. Reception)

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

Physical Location and Security

Do not allow unauthorised people into areas where personal or confidential data is kept unless supervised. Check peoples ID badges, especially if an unknown person is tailgating you into a secure area.

Take measures to prevent casual scanning of personal or confidential data such as security screens over desk tops.

Store personal or confidential data information in a locked drawer/filing cabinet.

Where transporting personal or confidential data a locked container/bag must be used. Items should be placed out of sight in the boot of a car. If taken home they should be stored securely at home in a secure place and should not be left in a car.

Reporting Possible Breaches of Security or Confidentiality

The Information Commissioner’s Office (ICO) has the power to conduct investigations into breaches of the Data Protection Legislation which can lead to an organisation having an information notice, an assessment notice or an enforcement notice, imposed upon them.

The ICO can also impose penalty notices on organisations based on two tiers the “higher maximum amount” up to €20m or 4% of total annual turnover, whichever is the greatest or the “standard maximum amount” up to €10m or 2% of total annual turnover, whichever is the greatest.

The ICO may impose the penalty notices if the organisation has seriously breached the Data Protection Legislation principles taking the following into account:

a) The nature, gravity and duration of the failure;
b) The intentional or negligent character of the failure;

c) Any action taken by the controller or processor to mitigate the damage or distress suffered by data subjects;
d) The degree of responsibility of the controller or processor;
e) Any relevant previous failures by the controller or processor;
f) The degree of co-operation with the commissioner, in order to remedy the failure and mitigate the possible adverse effects of the failure;
g) The categories of personal data affected by the failure;
h) The manner in which the infringement became known to the commissioner, including whether, and if so to what extent, the controller or processor notified the commissioner of the failure;
i) The extent to which the controller or processor has complied with previous enforcement notices or penalty notices;
j) Adherence to approved codes of conduct or certification mechanisms;
k) Any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, as a result of the failure (whether directly or indirectly);
l) Whether the penalty would be effective, proportionate and dissuasive.

Please refer to the Data Protection Act 2018 part 6 152 penalty notices for further information

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 personal, commercially confidential or special categories of personal data, e.g. the loss, theft or corruption of information, a network security breach, loss or theft of a computer, password misuse, etc. to the Data Custodian.
- Think carefully before sharing personal, commercially confidential or special categories of personal data without explicit consent, as staff will be held accountable for any unauthorised disclosure
- Do not open any suspicious emails. Report any possible cyber incidents to the SCW ICT Team
- Under the Data Protection Legislation where an incident is likely to result in a risk to the rights and freedoms of Data Subjects the ICO must be informed no later than 72 hours after the organisation becomes aware of the incident

If in any doubt, ask your line manager who may pass the query to the DPO, SIRO or the Caldicott Guardian

Monitoring Access to information containing personal, commercially confidential or special categories of personal data

Staff members should be aware that electronic systems that access, process or transfer data 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, commercially confidential or special categories of personal data is an offence and could lead to prosecution of individuals and/or the organisation.

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 that requires access to personal, commercially confidential or special categories of personal 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 SCW IG Manager, 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 SCW Registration Authority and SCW IG Manager 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 Smartcard or passwords
- Ensure that you accurately complete the necessary paperwork, provides suitable identification and attend 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 Legislation and Caldicott Principles, the Confidentiality Code of Practice and the Care Records Guarantee

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 data 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, Identification badge(s) and all relevant CCG equipment in compliance with the CCG leavers process
- All Information assets including hardware, software and smartcards must be recorded on an asset register that details the description, 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.

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 their 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 or SCW adopted IT 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 who can gain support from the SCW IG Manager. Any loss should be reported through the CCG Risk Management process.

<u>Remote Working and Portable Devices Best Practice Guidance</u>

- 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 unattended vehicles either on view 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/area. 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

<u>Passwords and Pin Codes</u>

- 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 recognised form
- **Regular password changes reduce the risk of unauthorised access to the machine and therefore passwords should be changed at least every 90 days, but more frequently if required**

USB/Portable Computing Devices

- Personal, commercially confidential or special categories of personal data must not be stored or transferred using any unencrypted "USB Memory" device
- Where it is not possible to encrypt data, the advice of the SCW 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 personal, commercially confidential or special categories of personal data 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 and the SCW IG 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
- Staff must not connect any personal or other devices not issued by the CCG to their portable devices

Use of the Internet

The internet is a limitless source of useful information which can facilitate learning and understanding and make the CCGs more efficient and productive. However, it is not without its dangers, such as illegal web-sites, unproven information and advice and information which are in breach of copyright control.

The CCG routinely monitors and audits access to the internet and will advise department managers of such use if deemed appropriate.

Access to the Internet is not allowed for any illegal or immoral purpose. No member of staff is permitted to access, display or download from Internet sites which hold offensive material.

To do so is considered a serious breach of CCGs' policy and may result in dismissal and, if appropriate, referral to law enforcement bodies e.g. child pornography.

Internet misuse may include but is not limited to accessing, disseminating, downloading or similar actions in respect of:

- pornography/'adult material',
- discrimination, harassment, libellous statements,
- chain letters, chat rooms
- share trading / money-making schemes,
- breach of confidentiality, copyright infringement
- Online gaming and gambling

- Music downloads (such as iTunes, etc)
- Excessive use of internet that is not work related

In addition, the following are only permitted if they are in direct support of CCGs' business, such as training, raising public health issues, etc; Guidance is available from the Information Governance Manager

- multimedia (such You Tube, etc) or internet based radio
- Social networking sites (such as Facebook, Twitter, MSN Messenger, etc)

Access to certain sites may be blocked.

Offensive material will be defined according to The CCGs' Bullying and Harassment Policy includes hostile text or images relating to gender, ethnicity, race, sexual orientation, religious or political convictions and disability. This list is not exhaustive. Other than instances which demand criminal prosecution, The CCGs are the final arbiter on what constitutes offensive material, and what is or is not permissible Internet access.

Users must not intentionally interfere with the normal operation of The CCGs' network, including propagating computer viruses, and generating high volume network traffic. Furthermore, any attempt to circumvent security measures in place or to connect a further internet connection will be considered under the disciplinary procedures

Users must not examine, change or use another person's files or output without the explicit permission of the originator.

Users must never access the internet using any other user's login details.

The downloading and installation of software is not permitted without the prior authorisation of IT Service desk.

Reasonable personal use of the system is not prohibited provided this does not interfere with the performance of your duties. Personal access to the Internet can be limited or denied by your manager who will determine what access is appropriate.

Users are responsible for adhering to the procedures and guidelines attached.

Users are also responsible, along with their managers, for ensuring they have the necessary skills and training to safely and appropriately use the internet and CCGs' hardware.

The CCG reserves the right to recover costs that are incurred irresponsibly.

Information Governance Mandatory Training

Every individual who works for the organisation is required to complete mandatory annual Information Governance 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 Data Protection Legislation principles and the risks to the reputation of the CCG which may occur if processes are not followed.

All staff are required to complete training using the NHS Data Security Awareness Level 1 modules provided by NHS Digital via the e-LfH platform, accessible through consultOD, or approved face to face training if offered.

The SCW IG Manager has conducted a training needs analysis and identified IG training which will need to be completed by those with additional job roles and functions.

If you are a new starter, temporary member of staff/contractor or have a query regarding training, please contact the SCW Information Governance Team via **scw.igenquiries@nhs.net** mailbox

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 and their eventual disposal. It is the requirement of the CCG 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 the following:

- All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)

Corporate Records can be considered records which contain the following:

- 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 form 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 Regulations Legislation 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
- Should demonstrate compliance with legal and regulatory requirements
- 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 securely 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 spread sheet to include who uses the file, location of where the file is situated and also retention review date
- Should the file contain personal, commercially confidential or special categories of personal data 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 (if patients records are retained NHS guidance is to include the individuals NHS number)
- Permission to access personal, commercially confidential or special categories of personal data should be restricted to a limited number of staff who requires 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 the Information Asset Owner, service leads and the SCW IG Manager.
- The above comes into effect where paper records are held, however where possible the organisation has an overarching paper light/paperless principle and therefore aims to minimise its paper records.
- There may be exceptions to the above in relation to HR and safeguarding/infection control records (likely personal identifiable/confidential) and contractual documentation (less likely personal identifiable/confidential). Further details are described within records management policy.

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 and archived
- 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 personal, commercially confidential or special categories of personal data should be controlled through the use of logins, password protection and encryption. Please review the CCG's Information Security Policy

What to do in the Event of Missing Corporate or Health Records

Missing records are a serious risk to the CCG 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 and folders (should the record be electronic)
3. Should the record remain missing after your search, you will need to contact the SCW Information Governance Team
4. Relevant staff should be made aware of the name of the record that is missing
5. The DPO, SIRO and Caldicott Guardian should be informed of the loss by the SCW Information Governance Team and advised of 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

Inform the Information Asset Owner (IAO) and SCW IG Manager if the records have been returned.

Any queries relating to lost records should be directed to the SCW Information Governance team via the scwcsu.igenquiries@nhs.net mailbox.

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.

Freedom of Information requests for the CCG are managed by the SCW FOI team.

How to Identify a Freedom of Information Request

Any member of the public (locally, nationally or globally) can ask to see information that is held by the SCW and any member of staff may be approached and asked for information under the FOIA.

The law requires the SCW 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:

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.

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 CCG's 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

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 in Section 4 of the CCG's 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

For all FOI questions and queries please email the CCG's FOI mailbox [insert details].

Business Continuity Plans

Business Continuity Management (BCM) is a method used to identify potential impacts that may threaten the operations of the CCG or the CCG itself. The fundamental element of business continuity is to ensure that whatever impacts the CCG the organisation continues to operate.

Business continuity plans (BCP) will help shape organisational resilience to 'threats', plan counteractions and minimise interruptions to the CCG 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 BCP's 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. The DC for each team will ensure the BCP's are made available to new and existing staff in their area.

For further information regarding BCP's please contact your teams DC, IAO or line manager.

Glossary of abbreviations

Abbreviation	Meaning
BCM	Business Continuity Management
BCP	Business Continuity Plan
CCG	Clinical Commissioning Group
CSU	Commissioning Support Unit
DC	Data Custodian
DPA	Data Processing Agreement
DPA 2018	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
DPO/DDPO	Data Protection Officer/Deputy Data Protection Officer
DSA	Data Sharing Agreement
e-LfH	E learning for health (online training provider)

FOI/FOIA	Freedom of Information Act 2000
FPN	Fair Processing Notification (privacy notice)
GDPR	General Data Protection Regulations
GP	General Practitioner
IAO	Information Asset Owner
ICO	Information Commissioners Office
IG	Information Governance
IT	Information Technology
SCW	South, Central and West
SIRO	Senior Information Risk Owner

Glossary of Terms

Commercially confidential Data/Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.
Controller	A controller determines the purposes and means of processing personal data. Previously known as Data Controller but re-defined under the GDPR. It owns data it collects from patients and which it may supply to others for processing.
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
Processor	A processor is responsible for processing personal data on behalf of a controller. Previously known as Data Processor but re-defined under the GDPR. A data processor (e.g. a CSU) does not own any data it processes when instructed by a data controller.
'Special Categories' of Personal Data	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature

	(d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Data Sharing Agreement (DSA) and Data Processing Agreement (DPA)	They are legally different terms but are frequently used interchangeably. It is important that all staff, not just the data protection experts, understand the difference. A **data sharing agreement** (or protocol) is a controller sharing data with another controller (or more than one other controller), for example a member practice shares data it owns with another organisation which also collects patient data which it in turn owns. Example – NHS organisations (practices, acute trusts, ambulance trust) sharing data they own into our "My Care Record" shared care records programme. A **data processing agreement** is controller to processor, for example a member practice shares identifiable patient data with SCWCSU – which does not own it – but processes it to provide the CCG with an aggregated analysis.

GDPR Conditions for Processing

Conditions for processing personal data	
Article 6, 1 (a)	The Data Subject has given explicit consent
Article 6, 1 (b)	It Is necessary for the performance of a contract to which the data subject is party
Article 6, 1 (c)	It is necessary under a legal obligation to which the Controller is subject
Article 6, 1 (d)	It is necessary to protect the vital interests of the data subject or another natural person
Article 6, 1 (e)	It is necessary for the performance of a task carried out in the public interest or under official authority vested in the Controller
Article 6, 1 (f)	It is necessary for the legitimate interests of the Controller or third party (can only be used in extremely limited circumstances by Public Authorities and must not be used for the performance of the public tasks for which the authority is obligated to do)
Conditions for processing special categories of personal data	
Article 9, 2 (a)	The Data Subject has given explicit consent
Article 9, 2 (b)	For the purposes of employment, social security or social protection
Article 9, 2 (c)	It is necessary to protect the vital interests of the data subject or another natural person where they are physically or legally incapable of giving consent
Article 9, 2 (d)	It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members

Article 9, 2 (e)	The data has been made public by the data subject
Article 9, 2 (f)	For legal claims or courts operating in their judicial category
Article 9, 2 (g)	Substantial public interest
Article 9, 2 (h)	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (see note below)
Article 9, 2 (i)	processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy
Paragraph 3 of the GDPR states that Personal data may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies. You must be able to demonstrate this if you are relying on this condition.	

Information Governance Staff Handbook

Please ensure you sign the accompanying slip confirming you have read and understood the information provided and return to the SCW IG Manager.

Should you have any questions or queries regarding information governance, please do not hesitate to contact the SCW Information Governance Team.

Your SCW IG Manager is

Paul Antony
SCW IG Team Mailbox: scwcsu.igenquiries@nhs.net

SCW IG Management Team

Beverly Carter – Head of Information Governance & Deputy Data Protection Officer

Judy McCarthy – Regional Information Governance Lead

Barry Thorp – Senior Information Governance Manager

Information Governance Staff Handbook email Confirmation text

When the handbook is circulated to staff, all are asked to that:

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

Reply emails shall include electronic signature. The reply returned to the CCG IG Lead, Data Protection Officer (or other staff member whom circulates it) shall also be date and time stamped.