NHS
Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

Data Protection Policy 2020 - 2022

Ratification Process

Lead Author	Corporate Services Manager (IG Lead) Corporate Services Support Manager (IG)
Developed by	Information Governance, Business Intelligence and IM&T Steering Group
Approved by	Information Governance, Business Intelligence and IM&T Steering Group – 23rd July 2020
Endorsed by	Integrated Performance and Assurance Committee (IPAC) – 30th September 2020
Ratified by	CCG Governing Body – 3rd November 2020
Version	2.0
Latest Revision date	July 2022 (or earlier if significant change to local or national requirements)
Valid on	30th September 2020

Document Control Sheet

Development and Consultation:	Policy developed from the previous version. The Policy required review to ensure it contained corrected references considering the General Data Protection Regulation (GDPR) implementation 25 May 2018. The CCG's IG, BI and IM&T Steering Group approved the document and it was endorsed by the Clinical and Management Executive Team (superseded by the Integrated Performance and Assurance Committee).
Dissemination	This Policy will be promoted throughout the CCG and uploaded to the public website.
Implementation	The Caldicott Guardian is responsible for monitoring the application of the Policy by ensuring that: • The Policy is brought to the attention of all employees. • Managers are aware of their responsibilities for ensuring that their staff implement the Policy. • Appropriate training and guidance is provided to staff. • Corporate business processes support the implementation of the Policy.
Training	Annual Data Security Awareness training is mandatory for all staff.
Audit	Annual Data Security and Protection Toolkit submission will provide assurance of compliance with this Policy.
Review	This policy will be reviewed bi-annually, or earlier if there are further changes in legislation, by the IG, BI and IM&T Steering Group.
Links with other documents	The Policy should be read in conjunction with the following CCG policies / procedures: • Confidentiality Code of Conduct for Employees • Access to Records Policy • Social Media Policy • Information Governance Policy and Management Framework • Information Security for Staff Policy (incl. Acceptable Use of Internet and Email) • Records Management and Lifecycle Policy • Staff Incident Reporting and Learning Procedure https://www.cambridgeshireandpeterboroughccg.nhs.uk/staff-homepage/guidance-and-information/information-governance/incident-reporting/ • Equality & Diversity Policy • Safeguarding Policies (particularly Adult Safeguarding Policy and Safeguarding Children Policy) • Safe Haven Policy • Cambridgeshire and Peterborough Health and Social Care Information Sharing Framework and supporting procedures (available on Cambridgeshire County Council website).
Equality and Diversity	An Equality & Diversity Impact Assessment was undertaken. The OD & HR Advisor (E&D Lead) confirmed that the document is compliant with the CCG Equality and Diversity Policy.

Revisions

Version	Page/Para No	Description of Change	Date Approved
1.0	New Policy	New Policy reflecting requirements of GDPR/updated UK Data Protection legislation. Subject Access Request and Access to Health Records procedures removed to become a standalone policy.	May 2018
2.0	Whole document	Bi-annual review and revision. Inclusion of additional appendices detailing Data Protection Principles; Lawful Bases for Processing and Individuals Rights under GDPR.	Sept 2020

Contents

1. Introduction

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG) is committed to the delivery of a first-class confidential service in accordance with the law, regulatory standards, and service user expectations. This means ensuring that all information is processed fairly, lawfully, and as transparently as possible so that patients and the public:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way we, as commissioner of publicly funded health and social care services handle information, and;
- understand their rights to access information held about them.

Confidentiality[1]: The four main requirements of confidentiality are:

- Protect – handle person-identifiable data securely.
- Inform – ensure that individuals are aware of how their information will be used.
- Provide choice – seek consent for use and/or disclosure of information wherever possible.
- Improve – seek better ways to protect, inform and provide choice.

Readers of this policy are encouraged to remember that we are all users of health and social care services and to consider the fairness, respect and confidentiality with which they would want their own records to be processed. It is impossible for policies to cover every eventuality and therefore readers should use reasonable judgement in decisions on using and communicating confidential information and ask for advice if needed.

2. Purpose and Scope

To ensure that all individuals to whom this policy relates are aware of their obligations and responsibilities regarding confidentiality, compliance with legislation and guidance and are aware of the consequences of breaches of confidentiality for individuals and for themselves.

To support readers' confidence in their day to day handling (processing) of personal data.

The Confidentiality and Data Protection Policy refers to 'readers'. Within this policy, this includes **anyone** who has agreed that they have a duty of confidence to the CCG and has access to CCG systems, or patient, staff and/or organisation-confidential or business sensitive information and will include but not be limited to all employees of CCG, partner organisations who access records systems, locums, students, volunteers and contractors.

This policy relates to the processing of person identifiable data and mainly refers to patient and service user information; however, the principles apply to any use of person-identifiable data (such as HR and staff data).

The principles of confidentiality also apply to confidential business activities (e.g. tendering processes, commissioning new services and performance management).

All readers must meet the standards outlined in this document as well as other relevant NHS Codes of Practice. They will have contracts of employment, professional registration

[1] From Confidentiality NHS Code of Practice, Department of Health 2003.

body regulations and further CCG policies and confidentiality agreements that they must sign up to.

3. Duties

The CCG is a commissioning organisation and The Health and Social Care Act 2012 determined limited purposes for a CCG to process patient identifiable data. Any requests for records should be referred to the Information Governance Team.

The following specific duties and responsibilities apply within the CCG:

- The Accountable Officer has overall responsibility for the Data Protection Policy.
- The Caldicott Guardian has responsibility for placing appropriate controls and procedures for monitoring access to any person identifiable data held by the CCG.
- The Information Governance (IG) Lead and Data Protection Officer (DPO), will be responsible for providing advice, liaising with other organisations to process subject access requests, co-ordinating the release of the data and investigating complaints and summary care record alerts.
- Managers at all levels are responsible for ensuring that staff for whom they are responsible are aware of and adhere to this policy.
- Information Asset Owners (Directors or Senior Responsible Officers (SROs)) are responsible for ensuring that all records that include person identifiable data are included in the directorate information asset register, are regularly reviewed (at least anually) and reporting any risks to the Senior Information Risk Owner (SIRO).
- Information Asset Administrators (IAAs) are responsible for ensuring that records containing person identifiable data are added to the directorate information asset register and that risks are reported to the Information asset owner (IAO).
- All staff including contractors, volunteers, agency staff and Governing Body members are responsible for person identifiable data that they record or process and are obliged to adhere to this policy.

4. Guidance

4.1 Data Protection Registration

The CCG has a responsibility to notify the Information Commissioner of the purposes for which they process data. The IG Lead manages the notification on behalf of Cambridgeshire and Peterborough CCG. Monitoring of the information asset register and data flow mapping will be carried out on an annual basis to ensure the registration is kept up to date.

4.2 Contracts and Service Level Agreements

The CCG must ensure that appropriate wording regarding compliance with the Data Protection Act is covered in all contracts and service level agreements before these are signed or changes are agreed. Temporary staff, students, volunteers and contractors are required to sign a confidentiality agreement. Copies are available from Reception staff at Lockton House, Cambridge. Other sites should contact HR to ensure agreed procedure is followed.

4.3 Training

All Staff must complete Data Security Awareness training on an annual basis. Compliance is monitored monthly and a reminder sent to those members of staff whose training is about to, or has, expired. The e-Learning for Health online training module entitled Data Security Awareness is utilised by the CCG. **https://portal.e-lfh.org.uk/**

4.4 Asset Register

All records containing person identifiable data should be identified in the directorate asset register and a lawful basis[2] for processing cited. This includes all data held in electronic and paper form. The asset register should be reviewed at least annually by the information asset administrators and updates reported to the information asset owners.

Systems, services and processes (paper based, and electronic) which process information should have a designated Information Asset Owner - IAO (and, in some cases, one or more Information Asset Administrators - IAAs). The role of the IAO is to understand what information is held within the system or is being transferred through processes, what is added and what is removed, methods of information transfer, and who has access to the system(s) and why.

4.5 Changes to systems and processes

It is important that changes to services and systems and processing of person identifiable data are assessed to ensure that confidentiality, accessibility, and integrity of data are maintained. Staff introducing changes must ensure that a Data Protection Impact Assessment (DPIA) is completed and approved before any changes are introduced especially where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is an assessment of the impact of the envisaged processing operations on the protection of personal data'.

4.6 Accuracy of data

All staff are responsible for ensuring that:

- Their own personal data in relation to their appointment is accurate and up to date
- Person identifiable data that they handle lawfully as part of their role is as accurate and up to date as possible, kept securely with restricted access and not kept for longer than necessary.

4.7 Emails

Staff should be aware that the Data Protection Act applies to emails sent or received for CCG purposes, including emails sent to private email addresses.

4.8 Security of Data

All staff are responsible for ensuring that personal or sensitive data is held securely and that it is not disclosed to any unauthorised third party. Data that is disclosed inappropriately or accidentally must be reported using Datix - the online incident reporting system. Major breaches of confidentiality or data loss should be reported to their line manager and the IG Lead/DPO in the first instance.

[2] **See Appendix 1** for the Six Lawful Bases for Processing Personal Confidential Data

4.9 Personal Data Breaches

Part 3 of the Data Protection Act introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority (Information Commissioner). Where feasible, incident reporting should be within **72 hours** of an organisation becoming aware of the breach.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, affected individuals must be informed without undue delay.

Organisations are required to have robust breach detection, investigation, and internal reporting procedures in place.

4.10 Retention of data

The Data Protection Act requires that data be not held for longer than necessary. Staff are required to identify the retention periods for all personal data held by them and ensure that it is disposed of securely in accordance with retention and destruction guidelines included in the Records Management Code of Practice for Health and Social Care 2016. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

4.11 Disclosure outside of the UK

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the UK to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects. Advice should be sought from the Information Governance Lead/Data Protection Officer or Caldicott Guardian before any such information is transferred.

5. Sharing Information

Please refer to the CCG Access to Records Policy for full details of when and how information sharing is appropriate/allowed, and responsibilities. For ease of use, this section provides a summary:

5.1 Sharing for direct care – consent model

In accordance with the Common Law Duty of Confidentiality, data protection legislation and various codes of best practice and conduct, the ideal situation when Personal Confidential Data (PCD) may be legitimately shared is that the person whose information it is (or their legal representative, e.g. parents for children, person with Power of Attorney for Health & Welfare) has freely given informed explicit consent to information being shared. Verbal consent is acceptable for direct care purposes (primary use) and must be recorded in the service user's record.

Consent is not the only lawful basis for sharing: Caldicott Principle 7; section 3 of the Health & Social Care (Quality & Safety) Act 2015 and (from 25 May 2018, General Data Protection Regulation Article 9(2)(h)) provide a lawful basis for sharing information with members of a service user's direct care team, for the sole purpose of providing them with care. This should not be defined as implied consent: the principle is one of reasonableness and 'no surprises' for the person whose information is being shared. Consent must not be obtained if there is no 'choice' except to share information. For example, if someone consents to a referral, then this can be understood as consenting to information being shared as relevant to that referral, and there is a lawful basis for this. Separate consent for sharing information should not be asked.

Individuals should always be informed about how their information will be shared. Continuing with the referral example, a clinician may tell the individual that they need to include information about other health conditions / co-morbidities as well as the health condition for the referral being made.

The CCG is a signatory to the Cambridgeshire and Peterborough Health and Social Care Information Sharing Framework containing an agreed Data Sharing Agreement template agreed with partner agencies. The overarching Framework and supporting documents are hosted by Cambridgeshire County Council. https://www.cambridgeshire.gov.uk/council/data-protection-and-foi/information-and-data-sharing/information-sharing-framework

Data Sharing agreements do not permit unrestricted access to PCD: they set the conditions for safe and secure sharing where there is a legitimate purpose for doing so.

5.2 Sharing without consent

Situations where consideration of disclosure of information without explicit consent include:

- Between health and social care professionals who are directly involved in the individuals' care for the purposes of provision of the highest quality care in accordance with principles section 6. *Note: All electronic sharing of personal confidential data should always be through a secure route i.e. NHS net to NHS net; encryption.*
- In the public interest – e.g. the Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988 requires the notification of certain diseases to the local authority.
- For the detection and prevention of serious crime or where it is necessary to fulfil a statutory obligation or court order. The Police do not necessarily have any legal right of immediate access to PCD. Please see the CCG Access to Records Policy for more detail.
- For safeguarding purposes – protection of a vulnerable child or adult from abuse or neglect. Refer to the CCG's Safeguarding Leads and policies.
- Where there is a risk of serious harm to an individual or others: health and safety issues for staff (e.g. environmental factors, violent patients) must be referred to the Local Security Management Specialist or Director of Governance as appropriate.
- Where the person lacks the capacity to make a particular decision to take a particular action for themselves, at the time the decision or action needs to be taken. This would include decisions about the sharing of information – see Mental Capacity Act 2005, Chapter 16: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/497253/Mental-capacity-act-code-of-practice.pdf

5.3 Access to records or sharing for non-direct care purposes (secondary use)

Service user information may need to be accessed or shared for non-care purposes. In some cases, (e.g. clinical audit, CQC quality inspections) there may be a lawful basis for staff and other authorised individuals to access records/PCD in accordance with performance and monitoring requirements in health and social care legislation.

In all other cases, if identifiable service user information for one or more users, is to be shared for non-care purposes, research and evaluation processes, or for any other non-care use (for example, service redesign), please refer to the CCG Access to Records Policy or Data Protection Impact Assessment Policy & Procedure.

In the event of any uncertainty or concern about sharing PCD the final decision on disclosure will be made by the Data Protection Officer (and/or the CCG's Caldicott Guardian, as appropriate).

5.4 National data opt-out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients can view or change their national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters.

By 2020 all health and care organisations are required to be compliant with the national data opt-out policy. NHS Digital and Public Health England are already compliant and are applying national data opt-outs.

6. Relevant Legislation and Statutory Best Practice

The **Common Law[3] Duty of Confidentiality** is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent unless there is an over-riding public interest (e.g. public health) or legal duty to do so (e.g. detection or prevention of serious crime[4]).

Article 8 of the European Convention of Human Rights, as brought into UK law by the Human Rights Act 1998, provides a right to respect for private and family life, subject to some restrictions that are 'in accordance with law' and 'necessary in a democratic society'.

Data Protection Act – DPA (2018) - The UK's third generation of data protection law received the Royal Assent, its main provision commenced on 25 May 2018. DPA 2018 replaced the Data Protection Act 1998. The new Act's aims were to modernise data protection laws to ensure they are effective in the years to come.

The overall principles of the GDPR are for organisations to be fair and transparent about how they use individuals' personal information, and for individuals, where possible, to have more choice and control over how their personal information is used. The GDPR built on current law and best practice ('evolution not revolution') and had little impact on most day to day care and safeguarding activities, where there is a clear lawful basis in GDPR to carry on sharing patient information, as at present.

Organisations that process PCD must register with the Information Commissioner's Office ('DPA Notification') on an annual basis. (See Section 4.1)

[3] Common law is based on society and cultural custom and judgements made in courts (case law) – it's not specifically recorded anywhere although many pieces of legislation use it as a basis. It is widely understood that we have a duty of confidence to service users: this is the common law of confidentiality, recognised in the Data Protection Act (1998) and other legislation.

[4] There is no one overarching definition of "serious crime". Section 115 of the Police and Criminal Evidence Act 1984 identifies "Serious Arrest able Offences" and the Information Commissioner's guidance on the Crime and Disorder Act 1998 gives advice on the data protection implications for data sharing; in some circumstances it may be necessary to seek legal advice.

Staff must follow the 7 key Data Protection Principles as set out under GDPR:

The Principles are listed in more detail in **Appendix 2**; the headings are as follows:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These Principles should lie at the heart of our approach to processing personal data.

Data protection legislation applies only to living individuals, who have a right to access information that an organisation holds about them (including, where it is held and who has accessed that information). A duty of confidence still applies to deceased individuals' personal information. The **Access to Health Records Act (1990)** confers the right of access to records of deceased patients to executors or administrators of a deceased person's estate and requests for access are administered in a similar way to requests for access to records under data protection law. Please see the CCG's Access to Records Policy for further information.

Individuals about whom information is held are known as data subjects. As well as the right of access, the GDPR provides the following rights for individuals:

- The right to be informed (usually known as a 'Fair Processing or Privacy Notice[5])
- The right of access
- The right to rectification
- The right to erasure[6];
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Individuals may also claim compensation for damages caused by a breach of the Act.

Individuals' Rights are explained in more detail in **Appendix 3**.

[5] CCG's Fair Processing Notice is available on the organisation's public website at https://www.cambridgeshireandpeterboroughccg.nhs.uk/search/?q=Privacy+notice

[6] Only inaccurate factual data may be removed from health records. If a service user disagrees with a clinical opinion, they may make an appropriate statement to that effect which can be added to their record – contact the IG Lead for advice in these circumstances.

The **Caldicott Principles** provide a framework for the use and sharing of confidential information. These are listed in full in **Appendix 4**; the headings are as follows:

1. Justify the purpose;
2. Do not use personal confidential data unless it is absolutely necessary;
3. Use the minimum necessary personal confidential data;
4. Access to personal confidential data should be on a strict need-to-know basis;
5. Everyone with access to personal confidential data should be aware of their responsibilities;
6. Comply with the law;
7. The duty to share information can be as important as the duty to protect patient confidentiality.

Following implementation of the Health and Social Care Act 2012, the Health and Social Care Information Centre published **A guide to confidentiality in health and social care**, which outlines 5 rules for confidentiality:

Rule 1 - Confidential information about service users or patients should be treated confidentially and respectfully.

Rule 2 - Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

Rule 3 - Information that is shared for the benefit of the community should be anonymised.

Rule 4 - An individual's right to object to the sharing of confidential information about them should be respected.

Rule 5 - Organisations should put policies, procedures, and systems in place to ensure the confidentiality rules are followed.

Finally, the NHS Care Record Guarantee, owned by the Care Quality Commission, places an emphasis on service user involvement with what is being recorded about them and how this information is used.

7. Policies, Procedures and References

- NHS Care Record Guarantee - https://digital.nhs.uk/media/329/Care-Record-Guarantee/pdf/Care_Record_Guarantee
- The NHS Code of Practice on Confidentiality (2003)
- 'A guide to confidentiality in health and social care' Health & Social Care Information Centre September 2013
- The Mental Capacity Act (2005)
- Access to Health Records Act 1990
- Caldicott Committee Report of the Review of Patient-Identifiable Information 1997
- The Information Governance Review ('Caldicott 2') April 2013
- Common Law Duty of Confidentiality
- Data Protection Acts 2018
- General Data Protection Regulation in force from 25 May 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Health & Social Care (Quality & Safety) Act 2015

8. Further Guidance

If you have any concerns or issues with the contents of this policy or have difficulty understanding how this policy relates to you and/or your role it is important that you seek clarification. Please raise concerns and queries with your line manager.

The Safeguarding Team can advise on safeguarding-specific queries.

The IG Team can advise on more complex situations and will consult with the Caldicott Guardian and Data Protection Officer as required.

Appendix 1: Lawful Bases for Processing Personal Data

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

More detail on each lawful basis can be found on the ICO's website at:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Appendix 2: Data Protection Principles

Lawfulness, fairness, and transparency

- Article 5(1)(a) of the GDPR says 'Personal data' shall be:
  processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency').

Purpose limitation

- Article 5(1)(b) says 'Personal data' shall be:
  collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

Data minimisation

- Article 5(1)(c) says 'Personal data' shall be:
  adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

Accuracy

- Article 5(1)(d) says 'Personal data' shall be:
  accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

Storage limitation

- Article 5(1)(e) says 'Personal data' shall be:
  kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Integrity and confidentiality (security)

- Article 5(1)(e) says 'Personal data' shall be:
  kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Accountability

There are two key elements. Firstly, the accountability principle makes it clear that Data Controllers are responsible for complying with the GDPR. Secondly, they must be able to demonstrate their compliance.

- Article 5(2) of the GDPR says:
  The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles].

Appendix 3: Individuals' Rights under GDPR

1. The right to be informed

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
- Individuals must be provided with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. This is referred to as 'privacy information'.
- Privacy information must be provided to individuals at the time we collect their personal data from them.

2. The right of access

- Individuals have the right to access their personal data.
- This is commonly referred to as subject access.
- Individuals can make a subject access request verbally or in writing.
- Organisations have one month to respond to a request.
- Organisations cannot charge a fee to deal with a request in most circumstances.

3. The right to rectification

- The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- Organisations have one calendar month to respond to a request.
- In certain circumstances organisations can refuse a request for rectification.
- This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).

4. The right to erasure

- The GDPR introduced a right for individuals 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.
- Organisations have one month to respond to a request.
- The right is not absolute and only applies in certain circumstances.
- This right is not the only way in which the GDPR places an obligation on organisations to consider whether to delete personal data.

5. The right to restrict processing

- 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, organisations are permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- Organisations 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).

6. The right to data portability

- 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 affecting its usability.
- Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
- The right only applies to information an individual has provided to a controller.

7. The right to object

- The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
- Individuals have an absolute right to stop their data being used for direct marketing.
- In other cases where the right to object applies, we may be able to continue processing if we can show that we have a compelling reason for doing so.
- We must tell individuals about their right to object.
- An individual can make an objection verbally or in writing.
- We have one calendar month to respond to an objection

8. Rights in relation to automated decision making and profiling.

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.

The GDPR applies to all automated individual decision-making and profiling.

Further information on Individuals' Rights under GDPR is available on the ICO website at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Appendix 4: Caldicott Principles

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised, and documented, with continuing uses regularly reviewed, by an appropriate guardian[7].

2. Do not use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

(Information Governance Review, Department of Health, March 2013)

[7] CCG's Caldicott Guardian is Carol Anderson, Chief Nurse

Initial Screening

Name of Proposal (policy/strategy/function/service being assessed)	Data Protection Policy
Those involved in assessment:	Policy developed in consultation with the IG, BI & IM&T Steering Group and initially endorsed by the Clinical Executive Committee (now superseded by the Integrated Performance and Assurance Committee)
Is this a new proposal?	The Policy required review to ensure it contained corrected references considering the General Data Protection Regulation (GDPR) implementation 25 May 2018. Updated in accordance with bi-annual review.
Date of Initial Screening:	06 June 2018

1. What are the aims, objectives?	This means ensuring that all information is processed fairly, lawfully, and as transparently as possible so that patients and the public: • understand the reasons for processing personal information; • give their consent for the disclosure and use of their personal information; • gain trust in the way we, as commissioner of publicly funded health and social care services handle information and; • understand their rights to access information held about them.
2. Who will benefit?	• All CCG staff • Data Subjects
3. Who are the main stakeholders?	Staff, Managers, IG, BI, IM&T Steering Group, Patients, service users
4. What are the desired outcomes?	To ensure that all individuals to whom this policy relates are aware of their obligations and responsibilities regarding confidentiality, compliance with legislation and guidance and are aware of the consequences of breaches of confidentiality for

	individuals and for themselves.
5. What factors could detract from the desired outcomes?	Lack of awareness of the existence of the Policy. Failure to follow the Policy/procedure.
6. What factors could contribute to the desired outcomes?	Knowledge of the Policy and Procedure Annual Training on handling personal data.
7. Who is responsible?	Staff, Managers, IG, BI, IM&T Steering Group
8. Have you consulted on the proposal? If so with whom? If not, why not?	Policy developed in consultation with the IG, BI & IM&T Steering Group endorsed by the Integrated, Performance & Assurance Committee.

9. **Which protected characteristics could be affected and be disadvantaged by this proposal (Please tick)**		Yes	No
Age	Consider: Elderly, or young people		x
Disability	Consider: Physical, visual, aural impairment, Mental or learning difficulties		x
Gender Reassignment	Consider: Transsexual people who propose to, are doing or have undergone a process of having their sex reassigned		x
Marriage and Civil Partnership	Consider: Impact relevant to employment and /or training		x
Pregnancy and maternity	Consider: Pregnancy related matter/illness or maternity leave related mater		x
Race	Consider: Language and cultural factors, include Gypsy and Travellers group		x
Religion and Belief	Consider: Practices of worship, religious or cultural observance, include non-belief		x
Sex /Gender	Consider: Male and Female		x
Sexual Orientation	Consider: Know or perceived orientation		x

What information and evidence do you have about the groups that you have selected above?

The above protected characteristics will have no adverse impact as the Policy was initially developed in accordance with new Data Protection legislation (i.e. General Data Protection Regulation May 2018) and is reviewed bi-annually to ensure continued compliance.

Consider: Demographic data, performance information, recommendations of internal and external inspections and audits, complaints information, JNSA, ethnicity data, audits, service user data, GP registrations, CHD, Diabetes registers and public engagement/consultation results etc.

How might your proposal impact on the groups identified? For example, you may wish to consider what impact it may have on our stated goals: Improving Access, Promoting Healthy Lifestyles, Reducing Health Inequalities, Supporting Vulnerable People

Examples of impact re given below:

a) Moving a GP practice, which may have an impact on people with limited mobility/access to transport etc

b) Planning to extend access to contraceptive services in primary care without considering how their services may be accessed by lesbian, gay, bi-sexual, and transgender people.

c) Closure or redesign of a service that is used by people who may not have English as a first language and may be excluded from normal communication routes.

Please list the positive and negative impacts you have identified in the summary table on the following page.

Summary	
Positive impacts (note the groups affected) N/A	Negative impacts (note the groups affected) N/A

Summarise the negative impacts for each group:

N/A

What consultation has taken place or is planned with each of the identified groups?

Policy was developed and approved in consultation with the IG, BI & IM&T Steering Group and endorsed by the Integrated, Performance and Assurance Committee

What was the outcome of the consultation undertaken?

Approval and Endorsement

10. **What changes or actions do you propose to make or take as a result of research and/or consultation?**

The Information Governance Team will be responsible for ensuring that this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Governing Body assurance in this respect.

10.1 **Will the planned changes to the proposal?**

	Please State Yes or No
a) Lower the negative impact?	N/A
b) Ensure that the negative impact is legal under anti-discriminatory law?	N/A
c) Provide an opportunity to promote equality, equal opportunity and improve relations i.e. a positive impact?	N/A

11. **Considering the views of the groups consulted and the available evidence, please clearly state the risks associated with the proposal, weighed against the benefits**.

Information risk The CCG must respect patient confidentiality in accordance with the NHS Constitution, HSCIC Guidance, and the Statutory Code of Practice. 'Necessity' is a qualifying condition to justify the lawful use of PCD within: (a) Regulation 7; (b) the Data Protection Act 1998; and (c) the Caldicott Principles.

12. **What monitoring/evaluation/review systems have been put in place?**

Audit will be undertaken by the Information Governance team. The Audit frequency will be yearly or more frequently if required.

13. **When will it be reviewed?**

July 2022

Date completed:	15th July 2020
Signature:	Lynn Carter, Information Governance Manager
Approved by:	Soomitra Kawal, OD & HR Advisor (E&D Lead)
Date approved:	16th July 2020