Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

Data Protection Policy 2018 - 2020

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
Ratified by	Clinical Executive Committee
Version	1.0
Latest Revision date	April 2020 (or earlier if significant change to local or national requirements)
Valid on	24 July 2018

Document Control Sheet

Development and Consultation:	Policy developed from the previous version. The Policy required review to ensure it contained corrected references in light of 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.
Dissemination	This policy will be promoted throughout the CCG and uploaded to the 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 Information Governance training is mandatory for all staff.
Audit	Annual IG 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: • Code of Conduct for Employees in respect of Confidentiality • Subject Access Requests and Access to Records Policy • Social Media Policy • Information Governance Management Framework • Information Security for Staff Policy (incl. Acceptable Use of Internet and Email) • Records Management Policy • 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 • Other (available on Cambridgeshire County Council website) Cambridgeshire and Peterborough Health and Social Care procedures.
Equality and Diversity	An Equality & Diversity Impact Assessment was undertaken. The Corporate Services Support Manager (E&D) 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 stand-alone policy.	May 2018

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.

The four main requirements of confidentiality[1] 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 with regard to 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).

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

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 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 Chief 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 Proection 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) 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 risks are reported to the Senior Information Risk Owner (SIRO).
- Information Asset Administrators 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.
- 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 information governance 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 legal basis 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 - IAA). 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 - formerly known as Privacy Impact Assessment (PIA)) is completed and approved before these are introduced.

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 using 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 the online incident reporting system Datix. Major breaches of confidentiality or data loss should be reported to their line manager and the IG Lead/DPO in the first instance.

4.9 Retention of data

The Data Protection Act requires that data is 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 Information Governance Alliance: 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/information-governance-alliance-iga

4.10 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 Subject Access Request and 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 legal 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 legal 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 legal 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/data-protection-and-foi/information-and-data-sharing/information-sharing-framework/

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 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 Subject Access Request and 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 Corporate Affairs 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 legal 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 Subject Access Request and Access to Records Policy or Privacy Impact Assessment guidance (from 25 May 2018 these will be known as Data Protection Impact Assessments).

In the event of any uncertainty or concern about sharing PCD the final decision on disclosure will be made by the CCG's Caldicott Guardian (and/or, from 25 May 2018, the Data Protection Officer, as appropriate).

6. Relevant Legislation and Statutory Best Practice

The **Common Law[2] 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 (eg public health) or legal duty to do so (eg detection or prevention of serious crime[3]).

[2] 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.

[3] 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

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'.

The **Data Protection Act – DPA (1998)** controls how an individual's personal information is used by organisations, businesses or the government. Organisations that process PID must register with the Information Commissioner's Office ('DPA Notification') on an annual basis. The CCG's IG Lead is responsible for the organisation's annual registration.

From 25 May 2018, the DPA will be repealed by the European Union General Data Protection Regulation (GDPR). 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. GDPR builds on current law and best practice ('evolution not revolution') and will have little impact on most day to day care and safeguarding activities, where there is a clear legal basis in GDPR to carry on sharing patient information, as at present.

Staff must follow the eight Data Protection principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purpose, and shall not be used for other purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of, or damage to personal data.
8. Personal data shall not be transferred outside the European Economic Area unless there is adequate level of data protection.

Data protection legislation (existing and future) 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 Subject Access Request and Access to Health Records Policy for further information.

Individuals about whom information is held are known as data subjects. As well as the right of access, the Data Protection Act gives data subjects the right to:

- be informed how an organisation uses their information (usually known as a Fair Processing Notice' or Privacy Notice[4])
- object to processing that is likely to cause or is causing damage or distress;
- prevent processing for direct marketing;

1998 gives advice on the data protection implications for data sharing; in some circumstances it may be necessary to seek legal advice.

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

- object to decisions being taken by automated means;
- in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed[5];
- claim compensation for damages caused by a breach of the Act.

The **Caldicott Principles** provide a framework for the use and sharing of confidential information. These are listed in full in Appendix 1; the headings are as follows:

1. Justify the purpose;
2. Don't 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.

[5] 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.

7. Policies and 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 1998; 2018 is a Bill in Parliament at time of writing
- 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: 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[6].

2. Don't 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)

[6] CCG's Caldicott Guardian is Karen Handscomb, Chief Nurse