HEALTHIER PEOPLE,
BETTER FUTURE

NHS
Heywood, Middleton and Rochdale
Clinical Commissioning Group

Data Security, Protection & Confidentiality Policy

Reference Number:	IG13
Version:	V1.2
Name/Department of originator/author:	Paul Fox Senior Information Governance Lead
Approval Committee	Information Governance Management Group
Date Approved	2nd October 2020
Ratified Body:	Information Governance Management Group
Review date:	2nd October 2021
Target audience:	All CCG employees, including Contractors, Agency workers and volunteers

DOCUMENT CONTROL

Policy Title:	Data Security, Protection & Confidentiality Policy
Policy Area	Information Governance
This policy Supersedes	N/A - replaces the Data Protection & Confidentiality Policy
Description of Amendment(s)	N/A
This document should be read in conjunction with:	All other IG / Data Security related policies
This document has been developed in consultation with:	GM Shared Services – People Services ☐ GM Staff Side ☐ Internal Auditors ☐ HMR CCG Staff ☐
Published by:	Heywood, Middleton and Rochdale Clinical Commissioning Group, Number One Riverside, Smith Street, Rochdale, OL16 1XU
Intended Audience:	All CCG employees, including Contractors, Agency workers and volunteers
Policy path location	SharePoint
Policy shared location	HMR CCG SharePoint

Document Approvals This document requires the following approvals:

Governance – Committee /Board/Other	Purpose	Outcome	Date
Information Governance Operational Group	Review and approval	Approved	16th May 2018
Corporate Governance Committee	Review and approval	Approved	12th December 2018
Information Governance Management Group	Review and approval	Approved	26th July 2019
Information Governance Management Group	Review and approval (via email and Chair's action)	Approved	2nd October 2020

Policy review control information

Version	Date	Reviewer Name(s)	Comments
Draft V0.1	*April 2018*	Lisa Winstanley / Chris Lawless (GMSS IG Team)	New Policy which replaces the Data Protection & Confidentiality Policy.
V.1	May 2018	Lisa Winstanley / Chris Lawless (GMSS IG Team)	Approved

V.1.1	July 2019	Paul Fox (Senior IG Lead)	Minor amendments to reflect operational changes
V.1.2	July 2020	Paul Fox (Senior IG Lead)	Annual review and amendments to provide more information on GDPR and DPA 2018 legislation

Contents

1. Introduction 5
2. Scope 7
3. The General Data Protection Regulation (GDPR) 7
4. The Data Protection Act 2018 11
5. Roles, responsibilities and Accountabilities 13
6. Conduct 15
7. The Duty of Confidence 16
8. The Caldicott Principles 17
9. Confidentiality Codes of Practice 18
10. Definitions of Personal Data & Special Categories of Data 19
11. Subject Access Request 19
12. Human Resources Information 19
13. Training and Awareness 20
14. Disciplinary 20
15. Equality Statement 21
16. Monitoring and Review 21
17. Legislation and Related Documents 22
18. Relevant Policies and Procedures 23

1. Introduction

1.1. The purpose of this Policy is to provide guidance to all Heywood, Middleton and Rochdale CCG (henceforth referred to as "the CCG") employees on Data Protection.

1.2. The CCG has a statutory duty to safeguard the confidential information it holds, from whatever source, that is not in the public domain. The principle of this policy is that no individual or company working for or with the CCG shall misuse any information or allow others to do so.

1.3. During the course of their day to day work, many individuals working within or for the CCG will often handle or be exposed to information, which is deemed personal, sensitive or confidential, (including commercially confidential) information. It is a requirement that any individual, company or other organisation to which this policy applies shall not at any time during the period they work for or provide services to the CCG nor at any time after its termination, disclose confidential information that is held or processed by the CCG.

1.4. All staff working in the CCG are bound by a common law duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the Data Protection Act 2018. (henceforth referred to as DPA) and, the EU General Data Protection Regulation (henceforth referred to as GDPR) and, for health and other professionals, through their own professions' codes of conduct.

1.5. The CCG understands the need for the strictest confidentiality in respect of data. This applies to manual and computer records and conversations about service users' treatments. Everyone working for CCG is under a legal and common law duty to keep service users' information, held in whatever form, confidential.

1.6. The Information Commissioners Office (ICO) can impose penalties upon the CCG, and/or CCG employees if non-compliance occurs.

1.7. Confidentiality can only be overridden in exceptional circumstances and with the appropriate justification and it must be fully documented.

1.8. The CCG will ensure that all personal service user and staff information is processed fairly, lawfully and as transparently as possible so that they can:

- Understand the reasons for processing personal information;
- Give their consent for the disclosure and use of their personal information where necessary;
- Gain trust in the way the CCG handles information;

- Understand their rights to access information held about them.

1.9. It is the policy of the CCG that all processing of personal information by or on behalf of the CCG, whether as a Data Controller or as a Data Processor for others, shall be in accordance with the requirements of:

- The Data Protection Act (DPA) 2018 and any subsequent amendments and statutory instruments;
- The General Data Protection Regulation (GDPR);
- The legal requirement to pay a data protection fee (under the Digital Economy Act 2017) to the ICO;
- The CCG's Policies and Procedures in relation to the protection and use of personal information;
- Processing personal information for deceased patients;
- The Access to Health Records Act 1990 and any subsequent amendments and statutory instruments.

1.10. The aims of this policy are:

- To safeguard all confidential information within the CCG;
- To provide guidelines for all individuals working within the organisation;
- To ensure a consistent approach to confidentiality across the CCG;
- To ensure all staff are aware of their responsibilities with regards to confidential information;
- To provide all individuals working within the CCG access to the documents which set out the laws, codes of practice and procedures relating to confidentiality and which apply to them.

These include:

- The Common Law Duty of Confidentiality;
- Caldicott Principles;
- Data Protection Act 2018;
- General Data Protection Regulation (GDPR);
- Health and Social Care Act 2012;
- Freedom of Information Act 2000;
- Human Rights Act 1998;
- Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures";
- The Public Interest Disclosure Act 1998;
- The Computer Misuse Act 1990;
- Data Protection (Charges and Information) Regulations 2018.

2. Scope

2.1. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority/honorary contract or work experience the organisations policies are also applicable whilst undertaking duties for or on behalf of the CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of the CCG.

2.2. For the purposes of this policy, confidential information shall include any confidential information relating to the CCG and/or its agents, customers, prospective customers, suppliers, patients (where processing has a legal basis) or any other third parties connected with the CCG and shall include without limitation:

- Service user information;
- Ideas/programme plans/forecasts/risks/issues;
- Trade secrets;
- Trusted methods and business design;
- Finance/budget planning/business cases;
- Prices and pricing structures;
- Sources of supply and costs of equipment and/or software;
- Prospective business opportunities in general;
- Computer programs and/or software adapted or used;
- Policy advice and strategy;
- Corporate or personnel information and;
- Contractual and confidential supplier information.

2.3. This is irrespective of whether the material is marked as confidential or not.

3. The General Data Protection Regulation (GDPR)

3.1. The General Data Protection Regulation (along with the Data Protection Act 2018) governs how we collect, store, process and share data.

3.2. Under GDPR, the CCG no longer must register with the ICO but under the Data Protection (Charges and Information) Regulations 2018 it is a legal requirement for data controllers to pay the ICO a data protection fee. These fees will be used to fund the ICO's data protection work.

3.3. The CCG, who is a Data Controller, must comply with the principles under GDPR the CCG is committed to compliance with the requirements of the DPA and GDPR and will ensure that all CCG employees and anyone providing a service on behalf of the CCG (directly employed and contractors) who have access to any personal data held by or behalf of the CCG or the Greater Manchester Shared Services (GMSS), are fully aware of and abide by their duties and responsibilities.

3.4. The CCG may be required by law to collect and use information about people with whom it works, including patients, public, employees, customers and suppliers. This personal information must be handled and managed appropriately, however it is collected, recorded and used and whether it is a manual or electronic record.

3.5. **Principles relating to the processing of personal data**

(a) Processed lawfully, fairly and in a transparent manner in relation to individuals;

The CCG must show transparency regarding how information is processed and the most common format of demonstrating this is via the production of a privacy notice. The CCG has a privacy notice available via the website which documents information processing activities.

(b) 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 not be considered to be incompatible with the initial purposes;

Only use personal information obtained by the CCG in connection with the business of the CCG and ensure information is not used for any purposes other than originally intended.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Only obtain the minimum amount of information and do not obtain information which is not needed.

(d) 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;

Ensure that all information entered either manually or electronically is accurate, and where recorded elsewhere ensure that there are appropriate procedures in place to continually review and update the different sources, to ensure accuracy and version control. Where possible, do not hold duplicate copies as this increases the risk of inaccurate information being held.

(e) 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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

All records are affected by this article regardless of the media within which they are held and/or stored. For further guidance please see the CCG's Records Management Policy. When disposing of personal information use only the confidential waste destruction process.

(f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The CCG and its IT provider have policies and processes in place to ensure the technical security of data. The IG Team has produced a variety of policies and procedures to inform staff regarding how to keep personal data secure and confidential. Please see the IG SharePoint page for more information. Some tips to help to do this are:

- Do not allow unauthorised access;
- Do not share passwords and ensure you lock your PC screen before moving away;
- Do not leave confidential information on your desk/fax or post trays and ensure all paperwork is tidied away when not in use or at the end of the day;
- Ensure that computer / laptop screens are locked when away from desk;
- Hold confidential conversations in a private area.

Article 5 (2)

"The controller shall be responsible for, and be able to demonstrate compliance with, the other data protection principles"

The CCG evidences compliance with this with the following:

- Implements and maintains a suite of data security, protection policies / procedures and guidance;
- Adopts a 'data protection by design and default' approach;
- Ensures GDPR compliant contracts are in place with organisations that process personal data on behalf of the CCG;
- Maintains a Records of Processing Activities (ROPA) – please see the Information Asset Register and / or the Data Flow Mapping Register located on SharePoint for more information;
- Implements and maintains appropriate security measures;
- Records and, where necessary, reports personal data breaches to the Information Commissioner's Office (ICO);
- Carries out data protection impact assessments (DPIA's) for uses of personal data that are likely to result in high risk to individuals' interests;
- Has an appointed Data Protection Officer;
- Adheres to relevant codes of conduct and signing up to certification schemes where appropriate.

3.6. **Rights of the Data Subject under GDPR**

3.7. Individuals have strengthened rights under GDPR. In summary, these are:

- **Right to be informed (Articles 13 & 14)** – Individuals have the right to be informed about the processing of their personal data, this is explained via the CCG Patients & Public & Staff 'Privacy Notices,'
- **Right of access (Article 15)** - Individuals can request access to personal data we hold about them (commonly called subject access). The timeframe for responding and supplying the information is 1 calendar month. No fee can be charged (unless an exemption applies).
- **Right to rectification (Article 16)** – Individuals can request that inaccurate personal data is rectified or completed if it is incomplete. The request can be verbal or in writing and the CCG have one calendar month to respond.
- **Right to restriction of processing (Article 18)** - Where accuracy is contested individuals have right to restrict processing. This is not an absolute right and only applies in certain circumstances. The CCG must respond to a request for restriction with within one calendar month.
- **Notification Obligation regarding rectification or erasure of personal data or restriction of processing (Article 19)** – The CCG (as data controller) must communicate rectification or erasure of personal data or restriction of processing to whom anyone whom the personal data has been disclosed (unless this is impossible or involves disproportionate effort).
- **Right to Data Portability (Article 20)** - This right only applies where explicit consent is used as the legal basis for any processing.
- **Right to object (Article 21)** – Individuals have the right to object to processing data. However, if the CCG can demonstrate compelling legitimate grounds to continue processing then it can continue.
- **Right not to be subject to a decision based solely on automated processing including profiling (Article 22)** - The CCG do not process data using this method, so this right will not apply to our data processing activities.
- **Right to withdraw consent (Article 7)** – Where consent is used as the legal basis the right to refuse (or withdraw) consent applies to information sharing. However, this right might not apply if the sharing is for a mandatory or legal requirement imposed on the CCG.
- **Right to complain (Article 77)** – If staff / patients feel that personal data processed at the CCG has not been handled correctly or are unhappy with a response to any requests made, a complaint can be made to the IT and Assurance team (initially) and the if still unhappy the complaint can be lodged with the Information Commissioner's Office (ICO) https://ico.org.uk/

3.8. For further information about individual rights under GDPR, please see the **Individual Rights Procedure document.**

4. The Data Protection Act 2018

4.1. The Data Protection Act 2018 (DPA) which sits alongside the General Data Protection Regulation (GDPR) plays a part in filling in the gaps that are not covered in the GDPR and where the GDPR permits member states to make some adaptations to reflect national requirements.

4.2. Under GDPR, the organisation no longer must register with the ICO but under the Data Protection (Charges to Information Regulations) 2018 it will remain a legal requirement for data controllers to pay the ICO a data protection fee. These fees are used to fund the ICO's data protection work the UK.

4.3. Schedule 1, Part 4 of the DPA 2018 (and also Article 30 of GDPR) states that the organisation shall maintain a Record of Processing Activities (ROPA) for personal data. Processing for the CCG is recorded on the Information Asset Register and Data Flow Mapping Register. An update on the current status of the CCG's record of processing is presented to the SIRO and the Information Governance Operation Group (IGOG).

4.4. Schedule 1, Part 4, Section 38 of the DPA states that an appropriate policy document needs to be in place for the processing of personal data carried out in reliance on a condition in Part 1, 2 or 3 of Schedule 1 of the Act. This is documented in the CCG 'Appropriate Policy Document' which sets out how we protect personal and special category data. The types of processing undertaken in the CCG where this is required are:

- Employment, social security and social protection - DPA 2018, Schedule 1, Part 1, S1;
- Part 2, S5 of Schedule 1 of the Data Protection Act 2018 where the processing of special category personal data is necessary for reasons of substantial public interest.

4.5. The DPA also covers the areas of processing which are not covered in the GDPR relating to:

Law Enforcement Processing

- It provides a bespoke means of processing personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes of, or access to, personal data transmitted, stored or otherwise processed;
- Allows the unhindered flow of data internationally whilst providing safeguards to protect personal data.

Intelligence Services Processing

- It ensures that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and Enforcement

- It enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.
- It allows the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.
- It empowers the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

4.6. **Section 170 of the Data Protection Act 2018**

4.7. Section 170 of the DPA builds on Section 55 of the DPA 1998 which criminalised knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data. The provision was most typically / commonly used to prosecute those who had accessed healthcare and financial records without a legitimate reason. This adds the offence of knowingly or recklessly retaining personal data (which may have been lawfully obtained) without the consent of the data controller.

4.8. **Section 171 of the Data Protection Act 2018**

4.9. Section 171 criminalises the re-identification of personal data that has been 'de-identified' (de-identification being a process such as redactions to remove / conceal personal data).

4.10. For example, using a method or system to reverse the redaction creating a new set of identifiable information.

4.11. **Section 173 of the Data Protection Act 2018**

4.12. Staff are reminded that under Section 173 of the DPA 2018 it is a criminal offence for the CCG or a person employed by the CCG to alter, deface, block, erase, destroy or conceal data with the intention of preventing disclosure of information that a data subject enforcing his / her rights would have been entitled to receive. Any member of staff taking such action would be liable on conviction to a fine.

4.13. For example, deliberately withholding or destroying information that if disclosed to a data subject as part of their request for access to their own data (right of access request) might cause embarrassment / damage to a member of staff or the CCG.

4.14. **Transfer of data outside the EU**

4.15. You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Please contact the Senior IG Lead if you are considering a transfer to an organisation/individual outside the EU.

5. Roles, responsibilities and Accountabilities

5.1. **Accountable Officer (AO)**

5.2. Although the Data Controller is the CCG, the Accountable Officer (AO) has overall accountability for the CCG's compliance with the Data Protection Act (DPA). The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian / SIRO / Data Protection Officer and designated staff such as the Information Governance Team. The AO shall ensure that the CCG resubmits an annual data protection notification and fee to the Information Commissioners Office.

5.3. **Caldicott Guardian**

5.4. The Caldicott Guardian will act as the conscience of the CCG and oversee all disclosures of patient information with particular attention being paid to extraordinary disclosures. The Caldicott Guardian will also ensure the CCG adheres to the 7 Caldicott principles.

5.6. **Senior Information Risk Owner (SIRO)**

5.7. The SIRO, under delegated authority from the AO will oversee compliance with the DPA and the development of appropriate policy and procedure. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

5.8. **The Data Protection Officer (DPO)**

5.9. The GDPR requires all public authorities to nominate a DPO. This role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance. The role involves:

- Advising colleagues on compliance;
- Training and awareness raising;
- Monitoring compliance and carrying out audits;
- Providing advice regarding data protection impact assessments;

- Being main contact point with the ICO;
- Maintaining expert knowledge in data protection.

5.10 **IT and Assurance Team (support provided by the Senior Information Governance Lead)**

5.11. The IT and Assurance Team will:

- Co-ordinate the Data Security and Protection Toolkit (DSPT) for the CCG;
- Manage the Information Governance Management Group (IGMG) agenda, items and minutes;
- Ensure the CCG pay the annual data protection fee to the ICO;
- Ensure that an appropriate Data Security and Protection Policies, associated procedures and guidance for the CCG is produced and maintained;
- Represent the CCG on Data Security and Protection matters;
- Act as a central point of contact on Data Security and Protection within the CCG;
- Ensure information governance incidents / data breaches are managed according to national procedures, monitored and are reported to the appropriate group/committee in conjunction with the Data Protection Officer;
- Report performance monitoring data on the handling of Subject Access Requests (SARs) and FOI requests received and processed including compliance with turnaround times;
- Facilitate appropriate and effective training to CCG staff when required;
- Carry out compliance checks;
- Maintain an Information Asset Register and Data Flow Mapping Register;
- Liaise with internal / external auditors regarding compliance with the DSPT / Data Protection / GDPR.

5.12. **Information Asset Owners (IAO's)/Administrators (IAA's)**

5.13. Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) are provided with training and support, and carry out information risk assessments regarding their information assets, Ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- Are responsible for the Information Asset assigned to them;
- Ensure that all personal data can at all times be obtained promptly from the Information Asset when required to process a SAR;
- Ensure that personal data held in the Information Asset is maintained in line with the CCGs Record Management Policy, specifically around maintaining the accuracy, validity and quality of the personal data. Any personal data when no longer required should be removed promptly in line with policy.

5.14. **Line Managers**

- All line managers have a responsibility to ensure that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Security and Protection;
- Where a breach of policy / procedure or near miss occurs, line managers will need to comply with the CCG Incident Management processes;
- Line managers will ensure that anyone providing a service on behalf of the CCG (directly employed and contractors) completes a confidentiality statement (Confidentiality Code of Conduct) before commencing employment.

5.15. **All Staff** (**this refers to all CCG employees including contractor / temporary staff and workplace students):**

- Adhere to this policy and all related procedures and processes to ensure compliance with the DPA /GDPR;
- Are subject to Data Protection compliance and accountable via personal liability;
- Have a responsibility to inform the IG Team of any new use or change of use of personal data immediately;
- Must maintain an appropriate level of awareness of the DPA / GDPR and to attend training as appropriate;
- Ensure that all personal information is accurate, relevant, up-to-date and used appropriately, for both electronic and paper Information Assets;
- Ensure that personal data is not removed from the CCG premises except where specifically required for the execution of legitimate functions of the CCG and, then, only in accordance with appropriate policies;
- Ensure that all copies of personal data output, or obtained from the system whether electronic, recorded on paper, or any other form, are securely and confidentiality managed and destroyed / erased when they are no longer required for CCG purposes;
- Ensure that the IG Team is advised as soon as possible of any problems or complaints relating to any individual rights under the Data Protection Act or unauthorised disclosures/ breaches of confidentiality;
- Failure to adhere to this policy and its associated procedures may result in disciplinary action, if an individual is subject to professional registration, referral to the appropriate regulatory body.

6. Conduct

6.1. Individuals shall not be restrained from using or disclosing any confidential information which:

- They are authorised to use or disclose by the CCG and/or;
- Has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure of an individual and/or;
- Has entered the public domain by an authorised disclosure for an unauthorised purpose by the individual or anyone else employed or engaged by the CCG and/or;

- They are required to disclose by law; and/or;
- They are entitled to disclose under the Public Interest Disclosure Act 1998 provided that the disclosure is made in an appropriate way to an appropriate person having regards to the provisions of that Act.

6.2. All individuals must:

- Exercise all due care and diligence to prevent unauthorised disclosure of confidential information;
- Ensure the physical security of all confidential documents and / or media, including storage of files on PCs. Confidential information must never be unattended and should be secure when not in use;
- Use password protection and not disclose passwords to anyone including work colleagues;
- Have regards to the provisions of that Act.

6.3. All individuals will be required to comply with this policy whilst working within the CCG and therefore for as long as the information remains confidential information. It is only when the information has entered the public domain that the information can no longer be classed as confidential.

6.4. If an individual is unclear if information should be classed as confidential, they must discuss the issue with their line manager / IG Team who will offer advice and guidance.

7. The Duty of Confidence

7.1. All NHS bodies and those carrying out functions on behalf of the NHS / CCG have a duty of confidence to service users and a duty to support professional ethical standards of confidentiality.

7.2. Everyone working for or with NHS / CCG records who handles, stores or otherwise comes across information that is capable of identifying individual service users has a personal duty of confidence to the service user and to his / her employer.

7.3. The duty of confidence is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

7.4. Service users expect that information given to them by their doctors, nurses and other members of the healthcare team is treated in confidence and not passed to others without their permission. Similar considerations apply to personal information concerning other individuals, such as staff. Particular care must be taken to avoid inadvertent or accidental disclosure. The underlying principle is that all information that can be related to an individual must be treated as confidential and it must not be communicated to anyone who is unauthorised to receive it. Unauthorised staff includes those who are not involved in either the clinical care of the service user or the associated administration processes.

7.5. No personal information, given or received in confidence, may be passed to anyone else without the consent of the provider of the information or with a legal / statutory duty. This is usually the service user but sometimes another person may be the source (e.g. relative or carer).

7.6. No personal information, given or received in confidence, for one purpose may be used for a different purpose without the consent of the provider of the information, unless there are exceptional circumstances or legal / statutory duty.

7.7. Service users are entitled to object to the use of their personal health data for purposes other than their direct care.

7.8. The duty of confidentiality owed to a deceased service user is consistent with the rights of living individuals.

8. The Caldicott Principles

8.1 Caldicott guidelines were introduced in response to concerns raised by the way the NHS was handling personal confidential data. As a result, in 1997 a committee was set up and lead by Dame Fiona Caldicott to investigate and produce guidelines to ensure the confidentiality of individual information. The committee came up with 6 principles known as Caldicott principles.

8.2 In 2013, there was a further review of the Caldicott framework, and a further report was produced called “Information Governance: To share or not to share” commonly known as Caldicott 3, this introduced a 7th Principle.

8.3 The Caldicott Principles are:

Principle 1 - Justify the purpose(s) for using confidential information

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.

Principle 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).

Principle 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.

Principle 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.

Principle 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.

Principle 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.

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

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.

9. Confidentiality Codes of Practice

9.1 In 2013 the Health and Social Care Information Centre produced a document entitled 'A guide to confidentiality in health and social care – Treating confidential information with respect'. This outlines 5 rules that organisations should adhere to in relation to handling information.

9.2 These are:

RULE 1: Confidential information about service user 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.

9.3 Further guidance on the above rules can be found in the guidance document at: https://digital.nhs.uk/article/1226/A-Guide-to-Confidentiality-in-Health-and-Social-Care-

10. Definitions of Personal Data & Special Categories of Data

10.1 **Personal Data**

10.2 Personal data is data that can identify an individual or with a combination of data items would identity an individual for example, name, address, postcode, date of birth, NHS number, National Insurance number etc. GDPR extends the definition of personal data to now include online identifiers and location data.

10.3 Information that identifies individuals is confidential and should not be used unless absolutely necessary.

10.4 Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. It should be noted however that even anonymised information can only be used for justified purposes.

10.5 **Special Categories of Personal Data**

10.6 The GDPR now refers to sensitive data as "special categories of personal data" (Article 9). These Special categories of data are:

- Racial or ethnic origin
- Political opinions
- Religious of philosophical beliefs
- Trade union membership
- Health Data
- Sexual life / sexual orientation
- Genetic data – introduced under GDPR
- Biometric data – introduced under GDPR

11. Subject Access Request

11.1. A Subject Access Request, (SAR), is a request from a data subject to view or obtain copies of personal data held about them by the organisation.
For further detail regarding the right of access please refer to the Individual Rights Procedure and the Information Rights Procedure: Information Access Process which are both located on SharePoint.

12. Human Resources Information

12.1. The CCG processes personal and special categories of personal data about its employees for example, sickness and occupational health records, performance reviews, equal opportunities monitoring,

12.2. The CCG takes all reasonable steps to ensure that the data it holds about staff is accurate, complete, current and relevant. Please inform HR / People Services if your personal details have changed. If a member of staff considers that data held on him / her is or may be inaccurate, or if he/she wishes to request access to such data, please contact the CCG SAR Lead.

13. Training and Awareness

13.1. The SIRO has the overall responsibility for ensuring that all staff are provided with adequate data security and protection training. This is provided via the national mandatory Information Governance e-training materials provided by NHS Digital. New staff members (including temporary, contractors) will be required to complete Information Governance e-learning training as part of their induction as well as a local induction to Information Governance with the IG Team.

13.2. Information Governance training is required to be undertaken by all CCG employees and those providing a service to the CCG. All NHS staff are mandated to undertake annual Information Governance mandatory training.

13.3. Where staff have specific and additional Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO, Information Asset Owners / Administrators additional Information Governance training will be required. Additional training will be made available to all persons, where it is required. For further guidance refer to the CCG IG Training Needs and Analysis (TNA).

13.4. To maintain staff awareness, the CCG will direct staff to several sources:

- Policy/strategy and procedures;
- Manuals;
- Line manager;
- Specific training courses;
- Other communication methods, for example, team meetings; website and CCG Newsletters.

14. Disciplinary

14.1. No employee shall knowingly misuse any information or allow others to do so.

14.2. Users must not access records/information that they have no legitimate reason to view, this includes records about themselves their family, friends, neighbours, acquaintances. If there is not a legitimate reason to access information users must not browse and should remember all transactions are auditable.

14.3. If an individual unintentionally divulges confidential information, or they are aware of any individual doing so, he or she must report it immediately to their line manager and / or to

the CCGs Senior Information Governance Lead.

14.4. Breaches of Data Protection and Confidentiality are a serious matter which could result in dismissal and / or prosecution. Please refer to the CCG Confidentiality Code of Conduct and the Disciplinary Policy which is located on SharePoint for further information.

15. Equality Statement

15.1 In applying this policy, the CCG aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

15.2 It considers the provisions of the Equality Act 2010 and promotes equal opportunities for all.

15.3 This policy has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. In carrying out its functions, HMR CCG must have due regard to the different needs of different protected equality groups in their area.

15.4 This applies to all the activities for which HMR CCG is responsible, including policy development and review.

15.5 **Due Regard**

15.6 The CCG's commitment to equality means that this policy has been screened in relation to paying due regard to the Public Sector Equality Duty as set out in the Equality Act 2010 to eliminate unlawful discrimination, harassment, victimisation; advance equality of opportunity and foster good relations.

16. Monitoring and Review

16.1 The CCG will undertake or commission assessments and audits of its framework, policies and procedures to monitor compliance and make improvements where identified.

16.2. This policy will be reviewed every two years and in accordance with the following on and as and when required basis if the following occurs:

- Legislative changes;
- Good practice;
- Guidance; case law;
- Significant incidents reported;
- New vulnerabilities; and

- Changes to organisational infrastructure.

16.3. Where there are no significant alterations required, this policy shall remain for a period of no longer than two years of the ratification date.

17. Legislation and Related Documents

17.1. Legal Acts:

- Data Protection Act 2018;
- General Data Protection Regulation 2018;
- Human Rights Act 1998;
- Freedom of Information Act 2000;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984;
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act (1990);
- Trademarks Act (1994);
- Terrorism Act (2000);
- Proceeds of Crime Act (2002);
- Money Laundering Regulations (2007);
- Criminal Justice and Immigration Act (2008);
- Environmental Information Regulations 2004;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2012;
- Human Rights Act 1998;
- ; Data Protection (Charges and Information) Regulations 2018;
- Care Act 2014;
- Children's Act.

Please note this list is not exhaustive.

17.2. Supporting Documents

- **Code of Practice on Confidential Information** 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/code-of-practice-on-confidential-information
- **A Guide to Confidentiality in Health & Social Care** 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/a-guide-to-confidentiality-in-health-and-social-care
- **The NHS Care Record Guarantee for England**
- **The Social Care Record Guarantee for England**
- **GMC Guidance on Confidentiality:**

https://www.gmc-uk.org/-/media/documents/confidentiality-good-practice-in-handling-patient-information---english-0417_pdf-70080105.pdf

- **BMA guidance on confidentiality:** https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records
- **The Caldicott Guardian Manual 2017:** https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
- **NHS Information Risk Management :** https://www.igt.hscic.gov.uk/KnowledgeBaseNew/DH_NHS%20IG%20-%20Information%20Risk%20Management%20Guidance.pdf
- **Records Management NHS Code of Practice for Health & 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
- **Data Security and Protection Toolkit (DSPT)**
- **The Report on the Review of patient-identifiable information (alternative title "The Caldicott Report") and the 'Information: To share or not to share? The Information Governance Review (also known as the Caldicott 2 Review)**
- **National Data Guardian "Review of Data Security Consent and Opt Outs" July 2016**
- **Government Response "Your Data, Better Security, Better Choice, Better Care" July 2017**
- **Department of Health "2017/18 Data security and protection for health and Social care organisations.**
- **IGA Guidance**: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga
- **ICO Guidance:** https://ico.org.uk/

18. Relevant Policies and Procedures

18.1. The following policies and procedures should be read in conjunction with this policy:

- Records Management Policy
- Information Risk Policy
- Information Security Policy
- Agile Worker Policy
- Freedom of Information Policy
- Secure Transfers of Data Procedure
- Data Security & Protection Breaches / Incident Reporting Procedure
- Information Rights Procedure / Information Access Process
- Individual Rights Procedure

- Confidentiality Code of Conduct
- Data Protection Impact Assessment / DP by Design – Compliance Checklist.