NHS
Bury
Clinical Commissioning Group

Data Protection and Confidentiality Policy

Version:	5.0
Ratified by:	NHS Bury Clinical Commissioning Group Information Governance Steering Group
Date ratified:	28 May 2021
Name of originator /author (s):	Information Governance Team
Responsible Committee / individual:	NHS Bury Clinical Commissioning Group Audit Committee
Date issued:	June 2021
Review date:	February 2023
Target audience:	NHS Bury Clinical Commissioning Group Members, staff, volunteers and contractors
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Data Protection and Confidentiality Policy CCG.GOV.010.5.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Information Governance Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Safe Transfer of Information Policy (haven).
This document has been developed in consultation with	NHS Bury CCG Information Governance Operational Group
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place Knowsley Street Bury BL9 0SN Tel: 0161 762 1500
Copies of this document are available from	CCG Corporate Office CCG website

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
0.1 = draft 1	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	26th September 2013
1.0 = Policy once ratified	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	9th March 2013
2.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	10th December 2014
3.0 = policy once reviewed	NHS Bury Clinical Commissioning Group, Quality and Risk Committee	15th November 2015
3.1 = policy once reviewed	GMSS IG Team	14th December 2017

4.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	30th January 2018
4.1 = policy review	IG Team	24th May 2021
5.0 = policy once ratified	NHS Bury Clinical Commissioning Group, Information Governance Steering Group	28th May 2021

Data Protection and Confidentiality Policy

Contents

1. Introduction and Aims

1.1. The purpose of this Policy is to provide guidance to all NHS Bury CCG (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 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 encounter during 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), the current 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 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 the public 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; and
- 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
- the current Data Protection registration of the CCG;
- 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;
    - Current General Data Protection Regulation;
    - 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.

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 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;
- business 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 Current Data Protection Act / General Data Protection Regulation

3.1. The Data Protection Act 2018 (DPA 2018) was enacted to supplement the requirements of the GDPR. It repealed DPA 1998 from May 2018. These acts and regulations dictate that information should only be disclosed on a need to know basis; they ultimately govern how we collect, store, process and share data. .

3.5. The CCG has registered with the ICO as a data controller. A data controller must comply with the eight principles of the current Data Protection Act (please refer to section 4 of this policy) and the articles of GDPR. The CCG is committed to comply 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 on behalf of the CCG , are fully aware of and abide by their duties and responsibilities of the Act and Regulation.

3.6. 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.

4. Data Protection Act (DPA) / GDPR Principles

4.1. The Data Protection Act 2018 is the UK's implementation of EU GDPR. It gives us a set of basic rules for good information handling. It requires transparency and accountability.

4.1.1. DPA makes provision about the processing of personal data. Most processing of personal data is subject to the GDPR.

4.1.2. Part 2 supplements the GDPR and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply

4.1.3. Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the law enforcement directive.

4.1.4. Part 4 makes provision about the processing of personal data by the intelligence services.

4.1.5. Part 5 makes provision about the information commissioner

4.1.6. Part 6 makes provision about the enforcement of data protection legislation.

4.1.7. Part 7 makes supplementary provision, including provision about the application of this act to the crown and to parliament.

4.2. The General Data Protection Regulation (GDPR) - The GDPR is led by some principles as stated in its Article 5.

4.2.1. (a) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals('lawfulness, fairness and transparency');

4.2.1.1. There is a requirement to make the public aware of why the NHS needs information about them, how it is used and whom it may be disclosed to. The CCG is obliged under the DPA, GDPR and Caldicott to produce a patient information leaflet / privacy notice.

4.2.2. (b) 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 not be considered to be incompatible with the initial purposes('purpose limitation');

4.2.2.1. 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.

4.2.3. (c) Personal data shall be Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed('data minimization');

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

4.2.4. (d) 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');

4.2.4.1. 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.

4.2.5. (e) 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 subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals('storage limitation');

4.2.5.1. 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.

4.2.6. (f) Personal data shall be Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures('integrity and confidentiality').

4.2.6.1. Examples of which 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.

4.3. Data Subject Rights

4.3.1. Data Subjects have enhanced rights under GDPR. In summary, data subjects still have the right to file a Subject Access Request (henceforth referred to as SAR) and obtain from the data controller a copy of their personal data, together with an explanation of the categories of data being processed, the purposes of such processing, and the categories of third parties to whom the data may be disclosed.

4.3.2. The GDPR expands upon this right, requiring data controllers to respond to SARs with additional information, including details of the period for which the data will be stored (or the criteria used to determine that period) and information about other rights of data subjects. One major change to SARs relates to the charging of fees. Under GDPR the organisation will be unable to charge a fee for the processing of SAR's.

4.4. Transfer of data outside the UK

4.4.1. You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Please contact the IG team if you wish to transfer to an organisation/individual outside the UK.

5. Roles, Responsibilities and Accountabilities

5.1. Accountable Officer (AO)

5.1.1. Although it is the CCG that is the data controller, the AO has overall accountability for the CCG's compliance with the DPA / GDPR. The development, implementation of, and compliance with this policy is delegated to the Caldicott Guardian/SIRO and designated Data Protection Officer. The AO shall ensure that the CCG resubmits an annual data protection notification and fee to the Information Commissioners Office.

5.2. Caldicott Guardian

5.2.1. The Caldicott Guardian will act as the conscience of the CCG and oversee all disclosures of patient information with attention being paid to extraordinary disclosures.

5.3. Data Protection Officer

5.3.1. The DPO is required as part of the changes to the DPA under the new regulation of GDPR. The DPO's role is to inform and advise the CCG and its staff about their obligations to comply with the GDPR and other data protection laws. They are required to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits. In addition, they are required to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc).

5.4. Senior Information Risk Owner (SIRO)

5.4.1. The SIRO, under delegated authority from the COO will oversee compliance with the DPA / GDPR and the development of appropriate policy and procedure. The SIRO will be advised by the Deputy Director Governance and Assurance and supported by the Information Governance Manager. The SIRO is responsible for ensuring any suspected breach is investigated and appropriate actions taken, and for managing information risk.

5.5. Information Asset Owners (IAOs)/Administrators (IAAs)

5.5.1. Under the responsibility of the SIRO:

- Information Asset Owners (IAOs) will be identified, provided with training and support and will carry out risk assessments on the information assets, to protect against unauthorised access or disclosure, within their area;
- will ensure the integrity of the information within their area and restrict the use to only authorised users who require the access;
- will be responsible for the Information Asset assigned to them;
- will ensure that all personal data can always be obtained promptly from the Information Asset when required to process a SAR;
- will 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.

5.6. Information Governance Manager

5.6.1. The Information Governance Manager will:

- manage and deliver Information Governance for the CCG;
- maintain an awareness of information governance issues within the CCG;
- review and update the information governance policy and any other relevant IG policy in line with local and national requirements providing template documents to the CCG;
- ensure that line managers are aware of the requirements of the Information Governance policy and any other relevant IG policy.

5.7. 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 the DPA / GDPR;
- 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 before commencing employment.

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

- Should adhere to this policy and all related Information Assets and processes to ensure compliance with the DPA / GDPR;
- are subject to DPA / GDPR compliance and accountable via personal liability;
- have a responsibility to inform the GMSS IG Team of any new 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 manual Information Asset;
- 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, microfilm, 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 Manager s advised as soon as possible of any problems or complaints

relating to any SAR or unauthorised disclosures/ breaches of confidentiality;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

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 who will offer advice.

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 can identify 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. 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. 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.

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

7.8. The duty of confidentiality owed to a deceased service user should be viewed as being consistent with the rights of living individuals.

8. Personal, Confidential and Sensitive Information

8.1. In accordance to GDPR personal data is any information that directly or indirectly relates to an identified or identifiable living person. It makes it clear that information such as an online identifier – e.g. an IP address – can be personal data. This definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

8.2. Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

8.3. Information that identifies individuals personally must be regarded as confidential and should not be used unless necessary.

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

8.5. Confidential information is information entrusted by an individual in confidence where there is a general obligation not to disclose that information without consent.

8.6. Confidential information may include personal information such as name, age, address, and personal circumstances, as well as sensitive personal information (as defined by the DPA / GDPR) regarding race, health, sexuality, etc.

8.7. Confidential information may be known or stored on any medium. Photographs, videos, etc. are subject to the same requirements as information stored in health records, on a computer, or given verbally.

8.8. The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). These categories are broadly the same as those in the DPA.

8.9. For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

8.10 Sensitive/confidential data under the terms of the DPA / GDPR includes but is not restricted to:

- information about a person’s racial or ethnic origin;

- political opinions;
- gender;
- religion and belief;
- membership of a trade union;
- sexual life;
- criminal convictions or charges;

9. Subject Access Request

9.1. A Subject Access Request, commonly referred to as a SAR, is a request from a data subject to see a copy of, personal information that is held about them as an organisation. All data subjects have the right (subject to exemptions) to access personal information which is kept about them by the CCG, both in electronic and paper files, this is known as a Subject Access Request (SAR).

9.2. Any individual is entitled to:

- Know what information is held about them and why;
- gain access to it regardless of the media which it is held;
- have their information kept up to date;
- require the CCG rectify/block, erase or destroy inaccurate information;
- not have processed confidential information about them likely to cause damage or distress;
- not have processed confidential information about them for the purposes of direct marketing.

9.3. In most cases the CCG will only process personal information with the consent of the data subject. If the information is sensitive, explicit consent may be needed. It may be a condition of patients, and employment of staff, that they agree to the CCG processing of specific classes of personal information.

9.4. The CCG may sometimes process information that by this definition is classed as sensitive. Such information may be needed to ensure safety or comply with the requirements of other legislation.

10. Freedom of Information

10.1. The Freedom of Information Act 2000 widens the scope of the DPA / GDPR as it also makes provision for personal data to be disclosed to third parties providing none of the DPA Principles / GDPR Articles are breached. Information generally will not be disclosed if to do so would be regarded as a breach of confidentiality or if it would cause distress to the data subject.

10.2. This Act allows public access to information held by Public Authorities. Public authorities include government departments, local authorities, the NHS, state schools and police forces. However, the Act does not necessarily include every organisation that receives public money, e.g. it does not cover some charities that receive grants and certain private sector organisations that perform public functions.

10.3. The Act does not give people access to their own personal data (information about themselves) such as health records or credit reference file. If a member of the public wants to see information that a public authority holds about them then they should make a Subject Access Request (SAR).

11. Disclosing Information

11.1. The CCG must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances the Police.

All staff and individuals providing a service on behalf of the CCG should exercise caution when asked to disclose personal data held on another individual to a third party. Where an individual is unsure as to the legitimacy of disclosing information, the IG Manager should always be consulted.

11.2. There may be times when personal data may be legitimately be disclosed, for example where:

- The individual has given their consent for information about them to be disclosed;
- the disclosure is in the legitimate interests of the provision of healthcare (e.g. if members of staff require the information to enable them to perform their jobs adequately or if there are justifiable patient safety concerns);
- the CCG is legally obliged to disclose the data.

11.3. The NHS Confidentiality: Code of Practice provides advice on using and disclosing confidential service user information and has models for confidentiality decisions and all staff should adhere to this guidance.

11.4. Personal information may be disclosed based on informed consent where the disclosure is necessary for healthcare purposes and is undertaken by a health professional or a person owing an equivalent duty of confidentiality.

11.5. The CCG will inform service users, staff and any other data subjects why, how and for what purpose personal information is collected, recorded and processed.

11.6. Consent of the data subject will be required where a disclosure of personal information is not directly concerned with the healthcare / treatment of a service user e.g. medical research, health service management, financial audit, personnel data or where disclosure is to a non-health care professional.

11.7. Under common law, personal information may be disclosed without consent for example:

- In order to prevent serious harm;
- where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the service user concerned and the broader public interest in the provision of a confidential service.

11.8. Where information is required by the police CCG staff should consult the SIRO and Information Governance Manager

12. Human Resources (HR) and Personnel Information

12.1. In keeping with good HR practice, the CCG retains and processes personal data on its employees. In addition, the CCG may from time to time, retain and process “sensitive personal data” as defined by the DPA / GDPR for example in relation to sickness and occupational health records, performance reviews, and equal opportunities monitoring for the prevention of fraud or other illegal activities.

12.2. The CCG takes all reasonable steps to ensure that the data it holds is accurate, complete, current and relevant. If a member of staff considers that data held on him/ her is or may be inaccurate, or if he/she wishes to have access to such data, then contact should be made with the HR department.

13. Training and Awareness

13.1. The SIRO has the overall responsibility for ensuring that all staff are made aware of the requirements of the DPA / GDPR and their IG obligations and this will be carried out by regular

mandatory Information Governance training sessions. Any new staff members (including temporary, contractors) will be required to complete Information Governance as part of their induction.

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 Data Security and Awareness training.

13.3. Where staff have specific Information Governance roles within the CCG i.e. Caldicott Guardian, SIRO etc. 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 Information Governance Training Needs and Analysis (TNA) document.

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

- Policy/strategy and procedure;
- Manuals;
- line manager;
- specific training courses;
- other communication methods, for example, team meetings; and staff Intranet.

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 CCG Information Governance Manager.

14.4. Breaches of Data Protection and Confidentiality are a serious matter and a breach of could result in dismissal and/ or prosecution.

15. Monitoring and Review

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

15.2. This policy will be reviewed every two years, and in accordance with the following on an 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.

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

16. Legislation and Related Documents

16.1. Legal Acts:

- Data Protection Act 2018;
- General Data Protection Regulation;
- Human Rights Act;
- Freedom of Information Act 2000;
- Thefts Act (1968 and 1978);
- Police and Criminal Evidence Act 1984 (PACE);
- 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;
- Access to Health Records Act 1990;
- Regulation of Investigatory Powers Act;
- Health and Social Care Act 2006 and;
- Human Rights Act 1998.

16.2. Supporting Documents

- NHS Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2017;
- NHS Information Risk Management;
- Records Management Code of Practice for Health and Social Care 2016;
- Data Security and Protection Toolkit;
- Caldicott 3.

17. Relevant Policies and Procedures

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

- Information Governance Policy;
- Records Management Policy;
- Information Risk Policy;
- Freedom of Information Policy;
- Acceptable Use Policy;
- Confidentiality Code of Conduct for staff;
- Secure Transfers of Information Procedure;
- Subject Access Request Procedure.