NHS
Wigan Borough
Clinical Commissioning Group

Data Security, Protection & Confidentiality Policy

DOCUMENT CONTROL PAGE	
Title	Data Security, Protection & Confidentiality Policy
Supersedes	Data Security, Protection & Confidentiality Policy (July 2019)
Minor Amendments	Reviewed and updated to reflect the UK GDPR and following the consultation in 2020 the Caldicott Principles re word and introduction of a new 8th Caldicott Principle. Inclusion of more detail around definitions and minor amendments made to ensure policy contains up to date information and links.
Author	Chris Lawless (Information Governance Manager)
Ratification	Approved at IGOG – August 26th 2021 Ratified at the Governance & Audit Committee – September 2021
Application	All Staff
Circulation	All Staff
Review	September 2023

Date Placed on the Intranet/SharePoint: Following Approval	**EqIA Registration Number** **16/13**

Contents

Introduction

1. The purpose of this policy is to provide guidance to all NHS Wigan Borough Clinical Commissioning Group (henceforth referred to as “the CCG”) employees on Data Protection.

2. The CCG has a statutory duty to safeguard the personal data, special category of data and other business confidential information it processes whatever format such as paper and electronic. The principle of this policy is to provide guidance regarding the legislation and key standards that the CCG and its staff and any other third party who works for or on behalf of the CCG must comply with to ensure data is confidential, available when needed and is of high integrity.

3. To support this policy the IG manager has produced a portfolio of policies, procedures guidance and templates, to help staff comply with key legislation including the UK General Data Protection Regulation (henceforth referred to GDPR) and the Data Protection Act 2018 (henceforth referred to as the DPA). Staff will also receive instruction and direction regarding this policy from a number of other sources including communications, team meetings and line management direction.

4. All staff working for or on behalf of the CCG are bound by a common law duty of confidentiality to protect all personal data they process during the course of their work.

5. This is not just a requirement of their contractual responsibilities but also a requirement of the DPA, GDPR and the National Data Guardian Data Security Standards and for healthcare and other professionals via their own professional Codes of Conduct.

6. The CCG is committed to adhering to data protection legislation and national standards. This means ensuring that all personal and special category data is processed fairly, lawfully, securely, efficiently and transparently so that the public can:

    - Understand the reasons for processing personal and special category data.
    - Gain trust in the way the CCG processes data / information.
    - Understand their rights regarding the processing of personal and / or special category data.

7. The CCG will continue to maintain and review policies, procedures and guidance to ensure compliance with data protection legislation, the 8 Caldicott principles and the 10 National Data Guardian Data Security Standards.

Purpose

8. This policy applies to those members of staff that are directly employed by the CCG and for whom the CCG has legal responsibility.

9. 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 also applies to all third parties and others authorised to undertake work on behalf of the CCG.

10. The purposes of this policy are:

    - To ensure personal data processed by the CCG adheres to confidentiality, availability and integrity.
    - To provide guidance for all individuals working within the organisation.
    - To ensure a consistent approach to data security and confidentiality across the CCG.
    - To ensure all staff are aware of their responsibilities with regards to processing personal data.

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

12. Everyone working for the NHS has a personal duty of confidentiality to the service user and to his / her employer. The duty of confidentiality is conferred by common law, statute, contract of employment, disciplinary codes and policies and professional registration.

Roles & Responsibilities

13. **Managing Director**

    The Managing Director's role:

    The Managing Director has ultimate responsibility for the implementation of the provisions of this policy. As the 'Managing Director" they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

14. The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

15. Responsibilities will be delegated to the:

16. **Caldicott Guardian**

The Caldicott Guardian's role:

- Ensures that the CCG satisfies the highest practical standards for handling patient identifiable information / confidential information.
- Acts as the conscience of the CCG.
- Facilitates and enables information sharing and provides advice on the options for lawful and ethical processing of information.
- Ensures that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Oversees all arrangements, protocols and procedures where confidential patient data may be shared with external bodies both within, and outside, the NHS.
- Attends appropriate annual training to ensure they remain effective in their role and to ensure the CCG comply with assertion 3.4.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

The Caldicott Guardian for the CCG is the Interim Chief Nurse.

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

The SIRO's role:

- Is an Executive Director or Senior Management Board Member.
- Takes overall ownership of the Organisations Information Risk Policy.
- Acts as champion for information risk on the Governing Body and provides advice to the Managing Director on the content of the Organisations Statement of Internal Control in regard to information risk.
- Understands the strategic business goals of the CCG and how other NHS organisations business goals may be impacted by information risks, and how those risks may be managed.
- Advises the Governing Body on the effectiveness of information risk management and data security across the CCG.
- Attends suitable annual training to ensure they remain effective in their role and to ensure the CCG comply with assertion 3.4.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

The SIRO for the CCG is the Director of Transformation & Sustainability / Deputy Chief Finance Officer.

18. **Data Protection Officer (DPO)**

The Data Protection Officer role:

- Informs and advises employees about their obligations to comply with the GDPR, the Data Protection Act and other relevant legislation and monitors compliance with such legislation;

- Monitors compliance with data protection policies and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, the production of a Data Security / IG Framework document supported by relevant policies and procedures.
- Raises awareness of data protection issues with staff and at a senior level.
- Raises awareness and monitors compliance of data security training.
- Monitors compliance of audits.
- Provides advice and guidance on any CCG Data Protection Impact Assessments (DPIA's) as per Article 38 of the GDPR.
- Maintains expert knowledge in data protection.
- Is the point of contact with the supervisory authorities, including the ICO, and any individual whose data is being processed.
- Attends suitable annual training to ensure they remain effective in their role and to ensure the CCG comply with assertion 3.3.1 of the Data Security & Protection Toolkit (NDG Data Security Standards).

The Data Protection Officer for the CCG is the Associate Director of Primary Care.

19. **Information Governance Manager**

The Information Governance Manager will:

- Deliver the Data Security (Information Governance) agenda for the CCG to ensure compliance with all relevant legislation, codes and guidance.
- Maintain awareness of Data Security / Information Governance issues within the CCG
- Oversee completion of the annual Data Security & Protection Toolkit(DSPT).

Review and update Data Security / Information Governance related policies / procedures / templates / guidance in line with local and national requirements.

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

The Information Asset Owners and Administrators will:

- Lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its patient population.
- Know what information comprises or is associated with each asset and understands the nature and justification of information flows to and from the asset.
- Know who has access to the asset, whether system of information, and why, and ensure access is monitored and compliant with policy.
- Ensure that any "system administrator" within their area has read, understood and signed the Confidentiality Code of Conduct IT / System Administrator disclaimer contained in Appendix B of the Confidentiality Code of Conduct.
- Understand and address risks to the asset and provide assurance to the SIRO.

21. **Line Managers**

Line Managers will:

- Take responsibility for ensuring that the Data Security, Protection & Confidentiality Policy is communicated and implemented within their team, group or directorate.

22. **Employees**

Employees will:

- Adhere to this policy.
- Undertake annual "Data Security Awareness" training as identified in the CCG Data Security Training Needs Analysis and where it is identified that further training and education is required / mandated staff will be informed via the Data Security Training Needs Analysis.

23. Definitions

Personal Data

24. Personal data means any information that contains details that identify living individuals even from one data item or a combination of data items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth, location data and online identifiers.

25. Personal data is confidential and should not be used unless absolutely necessary.

26. 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.

Special Category Data

27. Special category data is personal data that needs more protection because it is sensitive. This is personal data consisting of information as to: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions, biometric data and genetic data.

28. For more information about special categories of data please refer to the ICO guide at:https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data

Personal Confidential Data

29. This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence

Health Data

30. This means is personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Anonymous Data

31. This is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. GDPR does not apply to anonymised information and wherever possible anonymous data should be used. However, care must be taken to ensure the data is truly anonymous for example low numbers may make information identifiable.

32. **Pseudonymisation**

33. Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Processing

34. Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Controller

35. This means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor

36. This means a natural or legal person, public authority, agency or other body which processes personal data “on behalf of” the data controller.

Consent

37. Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal Data Breach

38. This means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The General Data Protection Regulation.

39. The EU GDPR became applicable in UK law from 25th May 2018 coinciding with the UK Data Protection Act 2018. Post the UK exit from the European Union the UK GDPR was introduced. The UK General Data Protection Regulation (along with the Data Protection Act 2018) governs how the CCG processes all personal data.

40. The GDPR applies to ‘Data Controllers’ and ‘Data Processors’ who process personal and / or special category data. It applies to automated and manual filing systems where personal data are accessible (e.g. chronologically ordered sets of manual records). Pseudonymised data e.g. key-coded data could also fall into the scope of GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

41. The GDPR states that you must have a lawful basis for processing personal or special category data. If processing personal data an article 6 condition is required. If processing special category data both an article 6 and an article 9 condition is required. Please see: Lawful basis for processing | ICO

42. Under the CCG no longer has to 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

The CCG as a Data Controller must comply with the 7 key data protection principles as set out in Article 5 (1) e of the GDPR. These are:

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

The CCG must be transparent regarding how personal data is processed. This is normally undertaken by the provision of a privacy notice. The CCG have a Staff Privacy Notice which is made available via SharePoint and a Patients & Public Privacy Notice which is available via the CCG website. Both of these Privacy Notices outline the CCG's data processing activities.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a matter 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 data 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 of which they are processed;

Only obtain the minimum amount of personal data and do not obtain personal data 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 personal data processed manually or electronically is accurate and up to date to ensure high quality data. Where personal data is provided from other sources 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 data 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 in so far as the personal data will be processed solely for archiving purposes in the public interests, 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*;*

For further guidance regarding records retention, please see the CCG's Records Management Policy. When disposing of paper personal data, all staff MUST use the

confidential waste destruction process. For the deletion / destruction of electronic data held on devices / equipment, please contact the IT provider.

(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. There is 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 to personal data.
- Do not share passwords with anyone.
- Do not leave confidential information on your desk 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 the desk.
- Hold confidential conversations in a private area.

The seventh principle Article 5 (2) states that:

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

Once again, transparency and accountability are key under GDPR. We must tell people what we do with personal data and be accountable for how we process this and thus is must be undertaken securely and confidentially at all times

The CCG evidence compliance with this as it:

- 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.

Rights of the Data Subject under GDPR

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

- ***Right to be informed (Articles 13 & 14)*** – Individuals the right to be informed about the processing of their personal data, this is explained via the CCG Patients & Public & Staff 'Privacy Notice/s,'

- ***Right of access (Article 15)*** – Individuals can request access to personal data we hold about them. The timeframe for responding and supplying the information is 1 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 month to respond.

- **Right to erasure (Article 17)** - Individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances.

- **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 IG team (initially) and the if still unhappy the complaint can be lodged with the Information Commissioner's Office (ICO) https://ico.org.uk/

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

The Data Protection Act 2018

43. 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.

44. 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).

45. 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. For more detail regarding this please refer to the Appendix 1 of the Appropriate Policy Document which is located on SharePoint.

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

47. **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.

48. **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.

49. **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.

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

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.

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

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

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

53. 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. An example of this is 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.

54. **Transfer of data outside the UK**

55. No data should be transferred outside of the UK without the express permission of the CCG SIRO and DPO.

    Please contact the IG manager (Chris.lawlesss@nhs.net) if you wish to transfer to an organisation / individual outside of the UK.

The Common Law Duty of Confidentiality

56. All NHS bodies and those carrying out functions on behalf of the NHS / CCG have a duty of confidentiality to patients and a duty to abide by professional ethical standards of confidentiality.

57. 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 confidentiality to the service user and to his / her employer.

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

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

Caldicott Principles

60. In 2013 the Caldicott Review was undertaken within the NHS and the Caldicott principles as highlighted below were created.

61. Information sharing for 'individual / direct care' is paramount to deliver the necessary care and treatment safely required, efficiently and effectively. The 8 Caldicott principles offer NHS staff guidance regarding how to achieve this whilst maintaining the confidentiality and security of personal data. There are also other important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

62. The principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes. The principles

are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names and addresses. In some instances, the principles should also be applied to the processing of staff information.

63. The 8 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 – Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3 – Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4 – Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5 – Everyone with access to confidential information should be aware of the responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6 – Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 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 confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators, and professional bodies.

Principle 8 – Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.

For more information re the Caldicott principles see:
https://www.gov.uk/government/publications/the-caldicott-principles

National Data Guardian Standards

64. The National Data Guardian Security Standards were proposed by the National Data Guardian (NDG) and agreed by the Government and Care Quality Commission (CQC) In 2017, the Department of Health and Social Care put in policy that all health and social care providers must follow the 10 Data Security Standards.

65. The Data Security Standards are:

Data Security Standard 1 (Personal Confidential Data)

All staff ensure that personal data is handled, stored and transmitted securely whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2 (Staff Responsibilities)

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3 - Training

All staff complete appropriate annual data security training and pass a mandatory test.

Data Security Standard 4 - Managing Data Access

All staff Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5 - Process Reviews

All Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6 - Responding to Incidents

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7 - Continuity Planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8 - Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9 - IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10 - Accountable Suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Conduct

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

- They are authorised to disclose.

- Has entered the public domain unless it enters the public domain as a result of an unauthorised disclosure of an individual.
- 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.
- They are required to disclose by law.
- 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.

67. 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.

68. 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.

Equality, Diversity & Human Rights Impact Assessment

69. The CCG is committed to promoting Equality, Diversity and Human Rights.

70. It is important to address, through consultation, the diverse needs of our community, patients, their carers and our staff. This will be achieved by working to the values and principles set out in the CCG's Equality, Diversity and Human Rights Strategic Framework.

71. To enable the CCG to meet its legislative duties and regulatory guidance, all new and revised procedural documents, services and functions are to undertake an impact assessment to ensure that everyone has equality of access, opportunity and outcomes regarding the activities. Contact the Governance Team for support to complete an initial assessment. Upon completion of the assessment, Governance will assign a unique EqIA Registration Number. The CCG undertakes Equality Impact Assessments to ensure that its activities do not discriminate on the grounds of:

- Age / Disability / Gender reassignment / Marriage and civil partnership / Pregnancy and Maternity / Race / Religion or belief / Sex /Sexual orientation.

72. Before any committee, group or forum validate a strategy, policy or procedural document an EqIA Registration Number will be required.

This policy has been impact assessed and the EqIA number is 16/13.

Consultation & Approval Process

73. This policy will be reviewed and approved by the Information Governance Group (IGOG) and ratified by the Governance & Audit Committee.

74. This policy will be reviewed every two years or when there are significant changes in the policy.

75. This policy will be monitored for effectiveness by self-assessment against any external accreditation that is applicable and may be subject to review by internal audit.

References & Bibliography

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Thefts Act (191968 and 1978)
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act (1988);
- Computer Misuse Act 1990
- Trademarks Act 1994
- Terrorism Act
- 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
- Digital Economy Act 2017 (Charges and Information) Regulations 2018
- Human Rights Act 1998
- Health & Social Care Act 2012
- Care Act 2014 / Children's Act 2004
- Department of Health's "Confidentiality: NHS Code of Practice" including supplementary guidance "Public Interest Disclosures"
- The Public Interest Disclosure Act 1998
  The Caldicott Guardian Manual**:** UK Caldicott Guardian Council - GOV.UK (www.gov.uk)
- NHS 'Confidentiality NHS Code of Practice
  https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- NHSX Information Governance Portal
  Information governance - NHSX
- Guide to the Notification of Data Security and Protection Incidents".
  https://www.dsptoolkit.nhs.uk/Help/29

- Records Management NHS Code of Practice for Health & Social Care 2016: Records Management Code of Practice 2020 - NHSX
- Data Security and Protection Toolkit (DSPT) Data Security and Protection Toolkit (dsptoolkit.nhs.uk)
- ICO Guidance : https://ico.org.uk/
- GMC Guidance on Confidentiality: Confidentiality - GMC (gmc-uk.org)
- BMA guidance on confidentiality: Confidentiality and health records toolkit (bma.org.uk)
- Code of Practice on Confidential Information Code of practice on confidential information - NHS Digital
- A Guide to Confidentiality in Health & Social Care: A Guide to Confidentiality in Health and Social Care - NHS Digital
- The NHS Care Record Guarantee for England

Associated CCG Documents

- CCG Records Management Policy.
- NHSx Records Management Code of Practice (adopted by the CCG).
- Data Security & Confidentiality Audit Procedure.
- Confidentiality Code of Conduct.
- Data Protection by Design Compliance Checklist.
- Data Protection Impact Assessment Template (full and short version).
- Data Quality Procedure.
- Data Security ((IG) Incident Reporting Procedure.
- Data Security Management Framework (IG Framework).
- Data Security Training Needs Analysis.
- Individual Rights Procedure.
- Rights of Access Procedure (SAR.)
- Information Sharing Agreement Template.
- Privacy Notice for Patients & the Public / Privacy Notice for Staff.
- Records Management Policy.
- Secure Transfer of Data Procedure.
- Acceptable Use Policy.