Bolton Clinical Commissioning Group

Confidentiality and Data Protection Policy

Policy Number	**IG002**
Target Audience	**CCG**
Approving Committee	**CCG Chief Officer**
Date Approved	**March 2020**
Last Review Date	**January 2020**
Next Review Date	**January 2022**
Policy Author	**IG Team**
Version Number	**V7.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1	September 2013	Approved	CCG Exec Team
1.1	January 2014	Andrea Hughes	Amendment to Section 3
	January 2014	IM&T Ops Board	Approved
1.2	November 2015	IG Team	Review document for approval
3.0	December 2015	IM & T Ops	Approved
4.0	January 2018	IG Team	Review document for approval, incorporating GDPR legislation
5.0	January 2018	IM & T Ops	Approved
6.0	February 2018	CCG Chief Officer	Approved.
6.1	January	IG Team	Reviewed
7.0	February 2020	IG Board	Approved
7.1	March 2020	CCG Chief Officer	Approved.

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1 Introduction

The purpose of this Policy is to provide guidance to all NHS Bolton Clinical Commissioning Group (referred to as "the CCG") employees on Data Protection.

The CCG has a statutory duty to safeguard the personal data, special category data and other business confidential information it processes, in whatever format, such as paper and electronic. The principle of this policy is to provide guidance on the Data Protection legislation and key standards that CCG staff, including any other third party working on behalf of the CCG, must comply with; ensuring data is of high integrity, remains confidential and is available when needed.

To support this policy the Information Governance (IG) team has produced a portfolio of policies, guidance, bulletins and templates, to help staff comply with key legislation including the General Data Protection Regulation 2016 (henceforth referred to GDPR) and the Data Protection Act 2018 (henceforth referred to as the DPA 2018). These IG documents are reviewed and updated on a regular basis. Staff will also receive instruction and direction regarding this policy from a number of other sources including communications, team meetings and line management direction.

All staff working in the CCG are bound by a Common Law Duty of Confidentiality to protect the personal data they process during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement of the GDPR, DPA 2018 and the National Data Guardian (NDG) Security Standards for healthcare and other professionals, through their own professions' Codes of Conduct.

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 as possible so that the public can:

- understand the reasons for processing personal and special category data;
- gain trust in the way the CCG processes data; and
- understand their rights regarding the processing of their personal and special category data.

2 Purpose

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.

The purposes of this policy are to:

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

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

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.

3 Accountability and Responsibilities

Chief Officer

The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Chief Officer" 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.

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.

Responsibilities will be delegated to:

Caldicott Guardian

The Caldicott Guardian's role:

- ensures that the CCG satisfies the highest practical standards for processing personal data, special category data and other business confidential information;
- facilitates and enables information sharing and advise on options for lawful and ethical processing of information;
- oversees all arrangements, protocols and procedures where confidential patient information 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).

For Bolton CCG, this will be Dr Jane Bradford, CCG Clinical Director.

Data Protection Officer

The Data Protection Officer's role:

- informs and advises CCG staff about their obligations to comply with the GDPR, the DPA 2018, other data protection 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 Governance and Safety, Mike Robinson.

Senior Information Risk Owner

The Senior Information Risk Owner's (SIRO) 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 Board and provide advice to the Chief Officer on the content of the Organisation's 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 Board on the effectiveness of information risk management across the CCG; and
- 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 Chief Finance Officer, Ian Boyle.

Information Asset Owners

The Information Asset Owners (IAO) (under the responsibility of the SIRO) role:

- leads and fosters a culture that values, protects and uses information for the success of the CCG and benefit of its patient population;
- knows what information comprises or is associated with each asset, and understands the nature and justification of information flows to and from the asset;
- knows who has access to the asset, the system of information, and why, and ensures access is monitored and compliant with policy;
- understands and addresses risks to the asset, and provide assurance to the SIRO.

Information Governance Manager

The Information Governance Manager's role:

- delivers the Data Security / Information Governance agenda for the CCG;
- maintains awareness of Data Security / Information Governance issues within the CCG;
- reviews and updates the Data Security / Information Governance related policies / procedures / templates in line with local and national requirements.

Line Managers

The Line Manager's role:

- takes responsibility for ensuring that their staff are compliant with, and working to, all relevant policy and procedure in relation to Data Protection the GDPR / DPA 2018 and any other relevant data protection legislation;
- where a breach of policy/procedure or near miss occurs, line managers will need to comply with the CCG Incident Management processes;
- ensures that anyone providing a service on behalf of the CCG (directly employed and contractors) completes a confidentiality statement before commencing employment.

All Staff

Staff's role:

- adheres to this policy and all related Information Assets and processes to ensure compliance with the GDPR / DPA 2018 and any other relevant data protection legislation;
- have a responsibility to inform the IG Manager of any new use of personal data immediately;
- maintains an appropriate level of awareness of the GDPR / DPA 2018 and to attend training as appropriate as identified by the Data Security Training Needs Analysis;
- ensures that all personal data is accurate, relevant, up-to-date and used appropriately, for both electronic and manual Information Asset;
- ensures 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;
- ensures 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;
- failure to adhere to this policy and its associated procedures may result in disciplinary action.

4 Definitions

Personal Data

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

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 Categories of Personal Data

Article 9 of the GDPR refers to sensitive data as “special categories of personal data”. This data is sensitive so needs more protection. These special categories of data are:

- Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health Data
- Sexual life / sexual orientation
- Genetic data
- Biometric data

Personal Confidential Data

Personal data including any health related information (including where health related information can be derived from context) or health related information in a context from which personal data can be identified, is personal confidential data. This term was introduced via the National Data Guardian Review of Data Security, Consent and Opts Outs conducted in 2013.

Health Data

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

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 where ever possible anonymous data should be used.

Pseudonymisation

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

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

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

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

Consent

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

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.

5 Data Protection Legislations

5.1 General Data Protection Regulation (GDPR) 2016

The General Data Protection Regulation (along with the Data Protection Act 2018) governs how the CCG processes personal data.

Under GDPR, the CCG no longer has to register with the Information Commissioners Office (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 on the CCG's network 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. The IG Manager has produced a variety of policies and procedures to inform staff regarding how to keep personal data secure and confidential. Please see the Polices section on the CCG website 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 the 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.

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) – the Information Governance Manager maintains the Information Asset Register and / or the Data Flow Mapping Register;
- 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.

5.2 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 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 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 available on the CCG's website.

5.3 The Data Protection Act 2018

The Data Protection Act 2018 (DPA 2018) 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.

Under GDPR, the organisation no longer has to 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.

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 Board.

The DPA 2018 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.

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.

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).

Section 173 of the Data Protection Act 2018

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.

Transfer of data outside the UK

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 of the UK.

5.4 The Common Law Duty of Confidentiality

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.

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.

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

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

5.5 Caldicott Principles

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

The 7 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 the 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.

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles.

5.6 National Data Guardian Standards

The National Data Guardian Standards were created from the third review undertaken by Dame Fiona Caldicott who is now known as the National Data Guardian for Health and Care. The review in 2016 made recommendations to the Secretary of State for Health aimed at strengthening the safeguards for keeping health and care information secure and ensuring the public can make informed choices about how their data is used. The NDG review outlines new data security standards for the NHS and social care, a method for testing compliance against the standards, and a new opt-out to make clear how people's health and care information will be used and in what circumstances they can opt out.

The full report is called Review of Data Security and Opt Outs, and can be accessed on the link below.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF

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.

6 Conduct

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

- They are authorised to process;
- 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.

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.

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

7 Training and Awareness

Data Security / 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 / Information Governance training as per the Data Security and Protection Toolkit.

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 Data Security / Information Governance Training Needs and Analysis (TNA) document.

To maintain high staff awareness the CCG will direct staff to a number of sources:

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

8 Disciplinary

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

Individuals 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.

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 Information Governance Manager.

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

9 Monitoring Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security and Protection Toolkit.

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

- legislative changes;
- good practice guidance;
- case law;
- significant incidents reported;
- new vulnerabilities;
- changes to organisational infrastructure.

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

10 References & Bibliography

- Data Protection Act 2018
- General Data Protection Regulation 2016

- 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
- 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 Social Care Record Guarantee for England
- The NHS 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 (also known as Caldicott 3)
- 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/

11 Other relevant Procedural Documents

- Records Management Policy
- Data Security Handbook
- Secure Transfers of Data Procedure
- Information Governance Policy
- Corporate Information Security Policy
- Disciplinary Policy and Procedure

This list is not exhaustive and further IG policies and procedures can be found on the CCG's website.