Arthington Medical Centre
5 Moor Road, Hunslet, Leeds, LS10 2JJ
0113 385 2180

CONFIDENTIALITY AND DATA PROTECTION POLICY

For Arthington Medical Centre

Equality Statement

This policy applies to all employees, Governing Body members and members of Arthington Medical Centre irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1. INTRODUCTION 4
2. AIMS 4
3. SCOPE 4
4. ACCOUNTABILITY AND RESPONSIBILITIES 5
5. DEFINITION OF TERMS 6
5.1 Personal data 6
5.2 Special categories of personal data 6
5.3 Direct Patient Care 6
5.4 Legal basis for processing identifiable data 7
5.5 Objections and Opt Out 7
5.6 Corporate Information 7
6. ENSURING INFORMATION IS SECURE AND CONFIDENTIAL 8
6.1 General Principles 8
6.2 Using and Disclosing Confidential Patient Information for Direct Healthcare 8
6.3 Using and Disclosing Confidential Staff Information 9
6.4 Using and Disclosing Corporate and Business Information 9
6.5 Information Security 9
6.6 Sharing Confidential Information Without Consent 10
6.7 Confidentiality and Conversations 10
6.8 Records Management 11
6.9 Access to Records 11
6.10 Information Sharing 11

6.11 Information Confidentiality Breaches 11
6.12 Privacy Impact Assessment/Data Protection Impact Assessment 12
7. CONFIDENTIALITY GUIDANCE AND LEGISLATION 13
7.1 General Data Protection Regulations (Regulation (EU) 2016/679) 13
7.2 Human Rights Act 1998 15
7.3 Common Law Duty of Confidentiality 15
7.4 Caldicott Principles 15
7.5 Information Commissioner's Office Codes of Practice 16
7.6 NHS Digital (formerly Health and Social Care Information Centre) Guidance 17
7.7 Information Governance Alliance (IGA) 17
7.8 The NHS and Social Care Record Guarantees for England 18
7.9 NHS Act 2006 18
7.10 Health and Social Care Act 2012 18
7.11 Health and Social Care (Safety and Quality) Act 2015 18
7.12 Computer Misuse Act 1990 18
7.13 Other legislation and guidance 19
8. TRAINING 20
8.1 Mandatory Training 20
8.2 Specialist Training 20
9. IMPLEMENTATION AND DISSEMINATION 20
10. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY 20
11. ADVICE AND GUIDANCE 21
12. ASSOCIATED DOCUMENTS (Policies, protocols and procedures) 21

1. INTRODUCTION

Arthington Medical Centre recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The Practice also recognise the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which they process, store, share and dispose of information.

Confidentiality and data protection legislation and guidance provide a framework for the management of all data from which individuals can be identified. It is essential that all staff and contractors of the Practice are fully aware of their personal responsibilities for information which they may come into contact with.

2. AIMS

The aim of the policy is to ensure that all staff understands their obligations with regard to any information they come into contact with in the course of their work and to provide assurance that the Practice have in place the processes, rules and guidelines to ensure such information is dealt with legally, efficiently and effectively.

The Practice will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of the General Data Protection Regulations (Regulation (EU) 2016/679) and the Data Protection Act and other associated and related legislation and guidance, contractual responsibilities and to support the assurance standards of the Information Governance Toolkit.

This policy supports the Practice in their role as providers of health services and will assist in the safe sharing of information with partner and agencies.

3. SCOPE

This policy must be followed by all staff that work for or on behalf of the Practice including those on temporary or honorary contracts, secondments, volunteers, pool staff, Governing Body members, students and any staff working on an individual contractor basis or who are employees for an organisation contracted to provide services to the Practice. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy covers:

All aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information

- Personnel/Staff information
- Organisational and business sensitive information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of, the organisation
- Practice information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Organisation, adoption or alteration of information
- Retrieval, consultation, storage/retention or use of information
- Disclosure, dissemination or otherwise making available information for clinical, operational or legal reasons
- Alignment, combination/linkage, blocking, erasing or destruction of information

Confidentiality and data protection within the practice is the responsibility of the data controller (owner/partners).

The Practice recognise the changes introduced to information management as a result of the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and where necessary referral to the appropriate regulatory bodies including the police and professional bodies.

4. ACCOUNTABILITY AND RESPONSIBILITIES

There are a number of key information governance roles and bodies that the Practice needs to have in place as part of its Information Governance Framework, these are:

- SIRO
- Governing Body
- Governance, Performance and Risk Committee
- Caldicott Guardian
- Information Asset Owner/Administrator
- Heads of Service/department
- All employees

The accountability and responsibility are set out in more detail in the Information Governance Strategy and Vision, Policy and Management

Framework which must be read in conjunction with this policy.

5. DEFINITION OF TERMS

The words used in this policy are used in their ordinary sense and technical terms have been avoided.

5.1 Personal data

Personal data refers to all items of information in any format from which an individual might be identified or which could be combined with other available information to identify an individual and is information which has a duty of confidence. This may include (but is not limited to):

- Name
- Date of Birth
- Post code
- Address
- National Insurance Number
- Photographs, digital images etc.
- NHS or Hospital/Practice Number
- Date of Death
- Passport Number
- Online identifiers and location data (such as MAC, IP addresses and mobile device IDs)
- Pseudonymised data

5.2 Special categories of personal data

Categories of information are classified as special categories of personal data require and additional safeguards when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Concerning health, sex life or sexual orientation
- Racial or ethnic origins
- Trade union membership
- Political opinions
- Religious or philosophical beliefs
- Genetic data
- Biometric data
- Records relating to criminal charges and offences

Special categories of personal data are also referred to as Personal Confidential Data (PCD), Sensitive Personal Data, Patient Identifiable Data (PID), Patient Identifiable Information (PII), confidential personal information (CPI) and personally identifiable information.

5.3 Direct Patient Care

The Caldicott Report (1997) defined direct patient care as:
"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care"

The Practice adheres to national guidance in relation to using Personal Confidential Data for healthcare purposes and recognises that such data can only flow where a clear legal basis enables this.

5.4 Legal basis for processing identifiable data

A Data Protection Impact Assessment (DPIA) is required in order to demonstrate a legal basis for processing identifiable data.

The DPIA references how people about how their data is being processed.

If a legal basis has been established in the first instance for processing identifiable data **and** the data is to be used for another purpose, explicit consent is required.

Explicit consent is described in GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, through a statement or clear affirmative action, signifies agreement to the processing of their personal data.

An overview of these considerations is provided within the Practice Privacy Notice.

5.5 Objections and Opt Out

Where patient identifiable information is being processed for purposes other than direct care, there is an obligation to respect opt outs that have already been presented.

The National Data Guardian suggested a new consent and opt out model within her report published in 2016. A new system for managing patient opt outs regarding the use of identifiable data for purposes other than direct care is being introduced.

5.6 Corporate Information

Corporate information includes:

- Governing Body and meeting papers and minutes
- Tendering and contracting information
- Financial and statistical information
- Project and planning information

Corporate information could be accessible through the Freedom of Information Act either from the Practice responding to a request for information or through making information accessible via the Practice Freedom of Information Publication Scheme. Where any corporate information has a duty of confidence attached to it - the information may be exempt from release. Additionally, other exemptions of the Act could restrict release of certain corporate information.

6. ENSURING INFORMATION IS SECURE AND CONFIDENTIAL

6.1 General Principles

- The Practice regards all identifiable personal information relating to patients as confidential and compliance with the legal and regulatory framework will be achieved, monitored and maintained.
- The Practice regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- The Practice will establish and maintain policies and procedures to ensure compliance with the General Data Protection Regulation, Data Protection Act, Human Rights Act, the Common Law Duty of Confidentiality, Privacy and Electronic Communications Regulations, the Freedom of Information Act and Environmental Information Regulations and other related legislation and guidance.
- Awareness and understanding of all staff, with regard to responsibilities, will be routinely assessed and appropriate training and awareness provided.
- Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate, effective and affordable confidentiality and data protection controls are in place.
- Where any disclosure of PCD is made there a must be a legal basis for doing so.

6.2 Using and Disclosing Confidential Patient Information for Direct Healthcare

There are clear legal bases in place when information sharing is needed for direct healthcare, however this still requires that patients be informed about:

- The use and disclosure of their healthcare information and records.

- The choices that they have and the implications of choosing to limit how information may be used or shared.
- The breadth of the sharing necessary when care is to be provided by partner agencies and organisations.
- The potential use of their records for the clinical governance and audit of the care they have received.
- Through a privacy notice outlining what information will be shared, the purpose of this, who the data will be shared with, how long data will be retained, the rights of the data subject (including opt-outs) and what security measures are in place to protect confidentiality.
- If not for direct care then explicit consent or some other legal basis must be present to enable sharing.

6.3 Using and Disclosing Confidential Staff Information

Processing of personal data where the information sharing is needed for direct communications related to their role, salary payment and pension arrangements, is lawful. Staff should be made aware that disclosures may need to be made for legal reasons, to professional regulatory bodies and in response to certain categories of freedom of information requested where the public interest in disclosure is deemed to override confidentiality considerations.

Using staff information for other purposes must be subject to explicit consent being granted unless another legal basis permits this.

6.4 Using and Disclosing Corporate and Business Information

All staff should consider all information which they come into contact with through the course of their work as confidential and its usage and any disclosure would be in line with agreed duties and for authorised work purposes.

Corporate information could be accessible through the Freedom of Information Act either from the Practice responding to a request for information or through making information accessible via the Practice Freedom of Information Publication Scheme.

6.5 Information Security

Rules and guidance on information security are set out in

- **The Information Security Policy** - sets rules, guidance and good practice on ensuring security of information in the workplace, on areas such as portable devices, email, paper and electronic systems.
- **The Records Management and Information Lifecycle Policy** – includes sections on transfer of, storage and archival of records.

6.6 Sharing Confidential Information without Consent

It may sometimes be necessary to share confidential information without consent or where the individual has explicitly refused consent. There must be a legal basis for doing so (e.g. To safeguard a child) or a court order must be in place. In deciding on any disclosure certain considerations and steps need to be taken:

- Discuss the request with the appropriate personnel such as the Caldicott Guardian and/or IG Lead.
- Disclose only that information which is necessary or prescribed by law.
- Ensure recipient is aware that they owe a duty of confidentiality to the information.
- Document and justify the decision to release the information.
- Take advice in relation to any concerns you may have about risks of significant harm if information is not disclosed.
- Follow any locally agreed Information Sharing Protocols and national guidance.

Requests may be received by other agencies which are related to law enforcement such as:

- The Police or another enforcement agency where the appropriate request form (in line with the Access to Records Procedure) needs to be submitted from the law enforcement agency in order for the Practice to consider the request.
- The Local and National Counter Fraud specialists in relation to any actual or suspected fraudulent activity.

Staff should also take into account the seventh Caldicott principle and Information Governance Alliance guidance if there is a clear legal basis to share.

6.7 Confidentiality and Conversations

Where during the course of your work you have conversations relating to confidential matters which may involve discussing (or disclosing information about) individuals such as patients or staff members you must ensure:

- Check individuals contact preferences
- Those discussions take place where they cannot be overheard.
- That for telephone calls the rule is you do not give out confidential information over the phone - unless you are certain as to the identity of the caller and they have a legal basis to receive such information (e.g. you may need to speak with another team member on the phone who is based at another location).

- Where you receive a request over the telephone for confidential information asks the caller to put the request in writing so details can be verified.
- That you do not discuss confidential work matters in public places or at social occasions.
- Where an answer phone is used ensure that recorded conversations on cannot be overheard or otherwise inappropriately accessed.

6.8 Records Management

The Practice has a Records Management and Lifecycle Policy which should be followed for all aspects of record creation, sharing, storage, retention and destruction of records.

6.9 Access to Records

Individuals have a right to request access to their records in line with the GDPR/Data Protection Act by making a Subject Access Request. All staff should familiarise themselves with the Practice access to records procedure which should be followed for all requests for personal data. This procedure also gives guidance in relation to requests for the records of deceased persons' under the Access to Health Records Act 1990 and for dealing with requests for information from the police.

Access to corporate information and records will be in accordance with Practice Freedom of Information Act and Environmental Information Regulations Policy.

6.10 Information Sharing

The Practice will ensure that information sharing takes place within a structured and documented process and in line with the Information Commissioner's Code of Conduct and in accordance with the Health and Social Care Act 2012 and Health and Social Care (Safety and Quality) Act 2015.

Any local Information Sharing Protocols that the Practice has signed up to need to be followed at all times, unless they conflict with law or statute.

6.11 Information Confidentiality Breaches

All actual, potential or suspected incidents involving breaches of confidentiality or cyber-related incidents must be reported on the Datix system following the Practice Incident Reporting procedure.

All incidents involving patient data should be reported to the Caldicott Guardian, who should consider whether serious breaches of confidentiality, or those involving large numbers of individuals, need to be reported to the

Information Commissioner via the Data Security and Protection Toolkit incident reporting tool in accordance with the Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.

Reportable breaches should be determined and presented within 72 hours of being identified.

What should be reported?

Misuses of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. The following list gives some examples of breaches of this policy which should be reported:

- Sharing of passwords and/or smartcards.
- Unauthorised access to the computer systems either by staff or a third party.
- Unauthorised access to personal confidential personal information where the member of staff does not have a need to know.
- Disclosure of personal data to a third party where there is no justification and you have concerns that it is not in accordance with the data protection principles and NHS Code of Confidentiality.
- Sending data in a way that breaches confidentiality.
- Leaving confidential information lying around in a public area e.g. photocopier.
- Theft or loss of patient-identifiable information.
- Disposal of confidential information in a way that breaches confidentiality i.e. disposing of patient records and or content of in an ordinary waste paper bin
- Processing identifiable information without an appropriate Information Asset and associated data flows being identified and recorded in the organisations register.

6.12 Data Protection Impact Assessment

All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns and risks a technique referred to as a Data Protection Impact Assessment (DPIA) must be used. A DPIA will assist to:

- Identify privacy risks to individuals
- Protect the Practice reputation
- Ensure person identifiable data is being processed safely
- Foresee problems and negotiate solutions
- Identify all Information Assets and corresponding data flows

The Practice procedure for DPIAs should be followed.

7. CONFIDENTIALITY GUIDANCE AND LEGISLATION

For personal and confidential Information held by the Practice there will be appropriate measures to ensure confidentiality and security, underpinning the principles of Caldicott, NHS Digital Guidance, ICO and professional Codes of Practice, legislation and common law.

7.1 General Data Protection Regulations (Regulation (EU) 2016/679)

The GDPR were adopted by the EU in May 2016 and was implemented in full on the 25 May 2018. The GDPR will replace the previous Directive 95/46/EC on which the Data Protection Act 1998 was based. All organisations must ensure they are fully compliant within the implementation period. The GDPR requires that data controllers ensure personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- 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
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- 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
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
- 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

It is important to note that the Regulation specifies that:

- organisations are accountable for how they handle personal data and need to develop and maintain adequate policies, procedures, processes and

systems to fulfil this role
- data processors can be held liable for breaches
- all actual information breaches must be reported via the IG Toolkit (to the ICO) within 72 hours of becoming known
- the penalty for breach of the Regulations is now capped at a maximum of €20,000,000 or 4% of the turnover of an organisation
- Organisations must employ the privacy by design approach to activities involving personal data. A Data Protection Impact Assessment is required for any project where personal data will be processed or flow or it is otherwise anticipated to have a high privacy risk
- fair processing notices must transparently explain how personal data is used and the rights of the data subject
- organisations outside of the EU are required to follow the principles of the Regulations if their customers/clients are based within the EU
- the consent model for processing personal data is to be further defined (see Caldicott 3 report and corresponding consultation and direction from the Department of Health)
- as part of the implementation of the Regulations, a register of data controllers, will no longer be maintained by the ICO
- data subjects have the new right to erasure, data portability, review of automated decision making and profiling, to request their personal data are removed when an organisation is retaining them beyond a reasonable or defined time period
- subject access requests must be completed within 30 days and provided free of charge (unless a request is “manifestly unfounded or excessive”)
- organisations must keep a record of processing activities
- appointment of a Data Protection Officer

The Data Protection Bill 2017 includes the national derogations of the GDPR and the implementation of Law Enforcement Directive (EU) 2016/680:

- The processing of personal data for law enforcement
- It defines which organisations are considered Public Authorities
- Process of reporting and potential consequences of data breaches
- The processing of personal data relating to children under the age of 13 years and the ability to seek the consent of children aged 13 years or older
- Role and powers of ICO and provision to charge fees
- Conditions for processing - listed
- Allowances for complaints and compensation, which can now include financial loss, distress and other adverse effects.
- Establishes new criminal offences: “knowingly or recklessly to re-identify information that is de-identified personal data”, data theft, unlawful obtaining of personal data and alteration of personal data in a way to prevent it being disclosed.
- Exemptions to the provisions of GDPR

7.2 Human Rights Act 1998

Article 8 of the Human Rights Act 1998 established a right to respect for private and family life, home and correspondence. This reinforces the duty to protect privacy of individuals and preserve the confidentiality of their health and social care records.

There should be no interference with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

7.3 Common Law Duty of Confidentiality

This duty is derived from case law and a series of court judgements based on the key principle that information given or obtained in confidence should not be used or disclosed further except in certain circumstances:

- Where the individual to whom the information relates has consented
- Where disclosure is in the overriding public interest; OR
- Where there is a legal duty to do so, for example a court order

The common law applies to information of both living and deceased patients.

7.4 Caldicott Principles

Dame Fiona Caldicott produced a report in 1997 on the use of patient information which resulted in the establishment of Caldicott Guardians across the NHS Structure. She was asked to conduct a further review and a new report: 'Information to share or not to share' was published in March 2013. The recommendations of this report have been largely accepted by the government and a revised set of Caldicott Principles were published:

1. *Justify the purpose(s)*
   every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented with continuing uses regularly reviewed, by an appropriate guardian.
2. *Don't use personal confidential data unless it is absolutely necessary*
   Personal Confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).
3. *Use the minimum necessary personal confidential data*
   where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. *Access to personal confidential data should be on a strict need-to-know basis*
   only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.
5. *Everyone with access to personal confidential data should be aware of their responsibilities*
   Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.
6. *Understand and comply with the law*
   every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.
7. *The duty to share information can be as important as the duty to protect patient confidentiality*
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the frameworks set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Caldicott Guardian also has a strategic and operational role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisation's overall governance framework. A detailed description of the Caldicott Function is given in the Information Governance Strategy.

In 2014, the post of National Data Guardian was established, with the role of helping to make sure the public can trust their confidential information is securely safeguarded and make sure that it is used to support citizens' care and to achieve better outcomes from health and care services.

7.5 Information Commissioner's Office Codes of Practice

The Practice processes data that is covered in the following Codes of Practice published by the Information Commissioner's Office (ICO):

- Data sharing
- Subject access
- Closed Circuit Television
- Privacy Notices
- Employment Practices
- Anonymization
- Personal Information Online
- Privacy Impact Assessments

7.6 NHS Digital (formerly Health and Social Care Information Centre) Guidance

This organisation was established in April 2013 and is responsible for facilitating the management and sharing of data across the NHS to support both operational and other functions such as planning, research and assessments.

Directions from NHS England allow NHS Digital to capture local healthcare information for commissioning purposes. To enable intelligent commissioning of healthcare services, NHS Digital collects, analyses, and processes healthcare data into a format that allows the appropriate commissioners access to the relevant data. In doing this, the Data Services for Commissioners programme allows commissioners access to the appropriate information without compromising patient confidentiality or statutory legal requirements surrounding the use of this data.

HSCIC (prior to NHS Digital) produced a Code of Practice: 'A Guide to Confidentiality in Health and Social Care' in September 2013:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of individuals.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

7.7 Information Governance Alliance (IGA)

The Department of Health, NHS England and NHS Digital have a statutory responsibility for producing advice and guidance relating to information governance in health and care. The IGA was formed to be the single authoritative source of information and guidance for the health and care sector.

The IGA also seeks to enhance the quality of health and care services, including people's experience of using those services, by improving information governance.

The IGA aim to improve information governance in health and care by:

- becoming the authoritative source of advice and guidance
- providing support to organisations to help them and their staff handle personal information confidently and in the best interests of people who use their services

- developing the leadership and culture of health and care services to promote legal and secure information sharing, and
- Developing the capacity and capability of information governance professionals, by providing expert advice and supporting knowledge sharing networks.

The IGA has produced a number of newsletters, guidance and responses to questions, which organisations should have due regard to.

7.8 The NHS and Social Care Record Guarantees for England

The NHS and Social Care Record Guarantees for England sets out the rules that govern how individual care information is used in the NHS and in Social Care. It also sets out what control the individual can have over this.

Individuals' rights regarding the sharing of their personal information are supported by the Care Record Guarantees, which set out high-level commitments for protecting and safeguarding service user information, particularly with regard to: individuals' rights of access to their own information, how information will be shared (both within and outside of the organisation) and how decisions on sharing information will be made.

7.9 NHS Act 2006

Section 251 of the NHS Act 2006 allows the Common Law Duty of Confidentiality to be set aside by the Secretary of State for Health in specific circumstances where anonymised information is not sufficient and where patient consent is not practicable.

7.10 Health and Social Care Act 2012

The Health and Social Care Act 2012 provides NHS Digital with a legal basis to process identifiable data and on behalf of other NHS organisations. The Act proves the authority to operate Data Service for Commissioners (DSfC) and Data Service for Commissioners Regional Offices (DSCROs).

7.11 Health and Social Care (Safety and Quality) Act 2015

The Health and Social Care (Safety and Quality) Act 2015 sets the expectation that information will be shared between health and social care in the interests of individuals. Individuals are able to override such sharing if they have an objection. The Act is seen as key to enabling the Caldicott principle of there being a duty to share between those health and social care professionals involved in the direct care of patients if it is in the best interests of those individuals.

7.12 Computer Misuse Act 1990

This Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

- Access data or programs held on computer without authorisation. For example, to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.
- Access data or programs held in a computer without authorisation with the intention of committing further offences, for example fraud or blackmail.
- Modify data or programs held on computer without authorisation.

7.13 Other legislation and guidance

In addition to the main legal obligations and guidance there are a wide range of Acts and Regulations which are relevant to Data Protection and confidentiality which may have an effect on disclosure and use of information (see list below). This is not an exhaustive list. Where you need any further guidance regarding any of the legislation or guidance listed - you can contact the organisation's Caldicott Guardianor the Information Governance lead (see section 11 Advice and Guidance).

- Abortion Regulations 1991
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Access to Medical Records Act 1988
- Audit & Internal Control Act 1987
- Copyright, Designs and Patents Act 1988 (as amended by the Copyright (Computer Programs) Regulations 1992
- Coroners and Justice Act 2009
- Crime and Disorder Act 1998
- Data Retention and Investigatory Powers Act 2014
- Digital Economy Act 2017
- Communications Act 2003
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
  Health and Social Care Act 2012
- Human Fertilisation and Embryology Act 1990
- Human Rights Act 1998
- Medical Act 1983
- Mental Capacity Act 2005
- NHS Digital. "FAQs on legal access to personal confidential data." Accessed 16 September 2016. Available from http://digital.nhs.uk/article/3638/Personal-data-access-FAQs.
- NHS Sexually transmitted disease regulations 2000
- Prevention of Terrorism (Temporary Provisions) Act 1989 & Terrorism Act

2000
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations 2000)
- Regulations under Health and Safety at Work Act 1974
- Road Traffic Act 1988
- The Children Act 1989 and 2004

All staff are bound by the codes of conduct produced by any professional regulatory body, by the policies and procedures of the organisation and by the terms of their employment contract.

The Department of Health Records Management Code of Practice sets out guidance for the creation, processing, sharing, storage, retention and destruction of records.

8. TRAINING

8.1 Mandatory Training

The Data Security Protection Toolkit requires that all staff must undergo information governance training annually. All staff will receive information governance in accordance with the IG Training Strategy.

Line managers must actively ensure that **all** staff undertake and complete the annual mandatory information governance training.

8.2 Specialist Training

Additional training may be provided in specialist areas such as data protection. The need for additional training should be identified with reference to the IG Training Strategy.

9. IMPLEMENTATION AND DISSEMINATION

Following ratification by the Quality and Performance Committee this policy will be disseminated to staff via an appropriate method e.g. the Practice intranet and communication through in-house staff briefings.

This policy will be reviewed every two years or in line with changes to relevant legislation or national guidance.

10. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY

An assessment of compliance with requirements, within the Data Security Protection Toolkit (DSP), will be undertaken each year. This includes confidentiality and data protection. Incidents are reported and all serious information governance issues are escalated appropriately.

Any suspicion of fraud or bribery should be reported at the earliest available opportunity through the Report NHS Fraud website or telephoning 08000 28 40 60.

11. ADVICE AND GUIDANCE

Advice and guidance on any matters stemming from the Policy can be obtained by contacting the CCG IG team:
leedscg.dataprotectionoffice@nhs.net

12. ASSOCIATED DOCUMENTS (Policies, protocols and procedures)

This policy should be read in conjunction with:

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Mobile Working Policy
- Risk Management Policy
- Incident Reporting Policy
- Business Continuity Plan
- Disciplinary Policy
- Anti-Fraud Policy
- Anti-Bribery Policy
- Whistle Blowing Policy
- Internet and Social Media Policy
- Email Policy

And their associated procedures (including but not limited to):

- Subject Access Request (Access to Health Records) Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- Privacy Impact Assessment Procedure and supporting documents
- Safe Transfer Guidelines and Procedure

This policy should also be read in conjunction with the Information Governance Handbook which provides guidance for staff on information governance compliance.