Data Protection Policy

Author:	Anne Bailey, Information Governance Manager
Document Owner:	Deputy Chief Executive, Gurjit Mahil and Head of Corporate Governance & Legal, Paul Mullane
Revision No:	10
Document ID Number	POLCGR007
Approved By:	Information Governance Group
Implementation Date:	July 2021
Date of Next Review:	July 2024

Best of care
Best of people

Data Protection Policy

Document Control / History	
Revision No	**Reason for change**
7	
8	Revised review date
9	Review post DPA 2018 and GDPR
10	Annual Review

Consultation
Information Governance Group June 2021
Caldicott Guardian

Data Protection Policy

Table of Contents

Data Protection Policy

To be read in conjunction with any policies listed in Trust Associated Documents.

1 Introduction

1.1 This document describes Medway NHS Foundation Trust (the Trust) policy on Data Protection (General Data Protection Regulations 2018); NHS Code of Confidentiality and Caldicott requirements, and employees' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and electronically.

1.2 The Trust holds and manages a great deal of personal and confidential information relating to patients, service users and carers, the public and employees of the NHS.

1.3 Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

1.4 The General Data Protection Regulation and Data Protection Act 2018 came into force on 25th May 2018 and replace the Data Protection Act 1998 which came into force on 1st March 2000. The Regulation/DPA is concerned with "personal and sensitive data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". It need not be particularly sensitive information; indeed it can be as little as a name and address.

1.5 The Regulation/DPA is divided to "Recitals" and "Articles" and works in two ways, giving individuals certain rights whilst requiring those who record and use personal information certain responsibilities. The Regulations incorporates the following principles which are binding for all organisations processing data:

1.6 Article 5 Principles relating to processing of personal data 1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate e 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

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

(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 ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by

this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

1.7 Failure to comply with GDPR legislation can lead to enforcement action from the Information Commissioners Office (ICO), including monetary penalty notices, claims for compensation or even criminal prosecution. The ICO enforces and oversees the GDPR and the Freedom of Information Act 2000.

2 Purpose / Aim and Objective

2.1 This document describes Medway Foundation Trust (the Trust) policy on the Caldicott Guardian principles, the common law duty of Confidentiality and the Data Protection legislation. It describes the responsibilities of each employee with regard to safeguarding patient's, staff and the Trust's confidential information held both manually (not electronic, in a structured filing system) and electronic (computer). This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and data security standards.

2.2 This policy establishes how compliance with GDPR will be monitored and that Information Asset Owners (IAO) will provide the Senior Information Risk Officer (SIRO) with timely, reliable and fit for purpose information to meet reporting requirements, to support legislative and regulatory compliance and to assist management in decision making.

2.3 The GDPR requires all public authorities to appoint a Data Protection Officer (DPO). The role of the DPO is to assist the Trust in monitoring internal compliance, inform and advise the Trust on its Data Protection obligations, provide advice regarding Data Protection Impact Assessments (of a which a policy can be found via QPulse and will act as a contact point for data subjects and the supervisory authority e.g. ICO. The Trust has appointed the Trust Secretary and Director of Corporate compliance and Legal service as the DPO. Should you need to contact the DPO please email medwayft.dpo@nhs.net or 07788916897

2.4 Assurances will be provided to the Caldicott Guardian, DPO and Trust Board through reports produced by the Information Governance Team. These reports will promote openness and transparency on how the Trust is complying with statutory duties and deadlines, and highlight key areas of risk and non-compliance.

2.5 The Trust aims to 'Be the BEST' in everything it sets out to do, and this extends to embedding Information Governance (IG) at the heart of how it protects, manages and uses patient, staff and corporate data.

3 Definitions

Data: Information which-

- is being processed by means of equipment operating automatically in response to instructions given for that purpose

- is recorded with the intention that it should be processed by means of such equipment
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system or
- does not fall within the above paragraph but forms part of an accessible record

Data Controller: 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 Flow: A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.

Data Processor: A natural or legal person, public authority, agency or other body which processes the data on behalf of the data controller.

Data Subject: An identified or identifiable natural living person to whom personal data relates

Direct Care: The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider.

Duty of Confidence: A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Explicit Consent: A form of consent normally given orally or in writing and is where the patient makes a clear and positive indication that they understand the consequences of what they are agreeing to and are content with these consequences.

Legitimate relationship: A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.

Patient: People who are users of the Trust's services, also known as 'Service Users' or 'Clients'.

Personal Data: Data that relates to and identifies a living individual that can identify the individual from this data or other information in the possession of the data controller. This is also known as Person Identifiable Data (PID).

Secondary Purpose: A purpose other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

Special Category Data: Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other philosophical beliefs, trade union membership,

genetic data, biometric data, physical or mental health condition, sex life or sexual orientation, criminal proceedings or convictions**.**

Processing: Any operation or set of operation 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.

Relevant Filing System: A structured set of information that can reference individuals either directly or indirectly.

Health Professional/Clinician: A individual registered by one of the professional organisations (GMC, NMC, HCPC) who provides health care services to a patient.

4 (Duties) Roles & Responsibilities

4.1 The Chief Executive (CE)

The Accountable Officer who is responsible for overall leadership and management of the Trust and has ultimate responsibility for ensuring compliance with the legislation. The Chief Executive is responsible for ensuring that the responsibility for data protection is allocated appropriately within the Trust and that the role is supported.

4.2 The Senior Information Risk Officer (SIRO)

The SIRO has overall responsibility for the organisation's Information Risk Policy and acts as the champion for information risk on the Board. This currently sits with the Director of IT Transformation

4.3 The Caldicott Guardian

The Caldicott Guardian is an advisory role established to protect the confidentiality of patient information and ensure it is shared appropriately and securely. This currently sits with the Medical Director.

4.4 Information Governance Manager and Data Protection Officer

Informs and advises the Trust and its employees of their obligations under the GDPR; monitors compliance with the GDPR and Trust policies; provides advice on DPIA's; cooperates with the ICO; acts as the point of contact for the ICO on issues relating to processing and other matters.

The IG Manager has a leadership role, maintaining the confidence of patients, staff and the public, through advice and guidance on the creation of robust and effective processes to protect and handle personal information.

4.5 IT Security Specialist

Provides advice on all aspects of electronic information security including Cyber security. Assesses the risks and threats and offers advice on controls to reduce the risks.

4.6 Directors

Are responsible for the local implementation of this policy in their areas of responsibility.

7.8 All Staff

Everyone working for the NHS has a legal duty to keep information about patients and staff confidential. They are required to adhere to confidentiality agreements in their contract of employment, the NHS Confidentiality Code of Practice, the Common Law duty of Confidence and any professional codes of practice issued by their professional body.

5 The Principles of the GDPR

The Trust is a public authority which collects and processes vast quantities of personal and special category data. As such we are required to abide by all relevant legislation pertaining to Data Protection and Confidentiality. The main legislation governing Data Protection are the GDPR (2016) and the DPA (2018) both of which have recently been enacted.

The principles of the GDPR will be discussed individually along with the measures the Trust must take to ensure compliance with the law.

Lawfulness, fairness and transparency

- Ensuring that the legal basis for the processing of information is identified before processing commences. – see appendix A
- As a public authority which processes personal and special category information, the legal basis for processing information for the provision of direct care is identified as Article 6 (1)(c) and/or 9(2)(h) – **See Appendix B Legal Basis for Processing.**
- Ensuring the Trust's Privacy Notice (available on the Trust website) is kept up to date, and complies with the Information Commissioner's Office (ICO) Code of Practice. The Trust must have an appointed Data Protection Officer, whose contact details are available to the public.
- Complying with the common law duty of confidentiality; that any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.

Purpose limitation – data is collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those

- A Data Protection Impact Assessment (DPIA) is completed for the introduction of new processes or the updating of existing processes for collecting personal information.
- The DPIA must contain the purpose of the collection along with the legal basis for processing. Information collected for one purpose may not automatically be used for a second purpose.
- The DPIA must be ratified by the Data protection officer before the new process or update can be applied.

Data minimisation – data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- Only data required for the specified legitimate purpose should be collected, nothing more.
- When completing a DPIA ask 'do I really need to collect this information; what does it add to my purpose?'
- Do not use person identifiable data when anonymous, pseudonymous or aggregate data will suffice.

Accuracy – every reasonable step must be taken to ensure that personal data is correct and up to date. Inaccurate data may need to be erased or rectified without

- The accuracy of the data recorded should be verified at every contact with the patient
- Data Quality Audits should be regularly undertaken to ensure that information recorded for the patient represents a true picture of their encounter with the Trust
- Inaccurate demographic data should be corrected immediately without delay. Inaccurate clinical data should not be erased if it forms part of the patient's hardcopy record. Follow guidance in the Health Records Management policy for appropriate correction techniques. Inaccurate electronic data may be erased, as long as the system records this access and action.
- If a clinician has acted on the inaccurate data, then the inaccurate data should not be erased. A comment should be added to the patient record and the inaccuracy highlighted.

Storage limitation – data should be kept for no longer than necessary

- All staff responsible for the storage of patient personal information (electronic or hard copy) should follow the Records Management Code of Practice for Health and Social Care 2016 with regards to retention periods.

- All staff wishing to destroy personal data should contact the Health Records Manager, or the Information Governance to discuss the method of destruction.

Integrity and confidentiality – protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

- All hardcopy personal information must be protected against inappropriate access. All staff must adhere to the 'Secure Transfer of Information policy'.

- Routine IG Compliance checks should be carried out by ward managers/matrons quarterly and results sent to the IG department.

- Random unannounced IG Compliance checks will be undertaken by the IG Team and as part of the perfectapp ward round.

- All electronic systems which store personal information should follow the Trust's IT Security Policy

Rights of individuals: There are 8 rights which every individual has under GDPR in relation to their personal data:

- The right of access – the right of patients to know what the Trust is holding about them. This is also known as the right of subject access and is managed by legal services medwayft.sars@nhs.net
- The right to be informed – this is provided using privacy notices and patient leaflets. The Trust's privacy notices and leaflets can be found here [https://www.medway.nhs.uk/about-us/privacy-policy.htm.
- The right to rectification – this allows individuals to have inaccurate personal data (a "statement of fact") rectified or completed if it is incomplete. This is normally completed by the clinical teams.
- The right to erasure – this right is not used in the NHS as all information needs to be kept for a clinical or legal reason. For further information please contact medwayft.dpo@nhs.net
- The right to restrict processing and object to processing of data – this is part of the National opt-out programme more information can be found on our website. .
- Rights in relation to automated decision making and profiling – at this time the Trust does not completed automated processes for patients or staff.

CONFIDENTIALITY

Health information which is collected from patients in confidence attracts the common law duty of confidentiality until it has been anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

The 'Confidentiality: NHS Code of Practice' was published by the Department of Health and is a guide to required practice for those who work within or under contract to NHS organisations. The Code is relevant to anyone working in and around the health services.

The importance of maintaining confidentiality can be evidenced by its inclusion in all NHS staff employment contracts, in the NHS standard Terms & Conditions for procurement and in Codes of practice published by professional bodies such as the NMC, the GMC and the HSPC.

MFT is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their individual needs and does not discriminate against individuals or groups on any grounds.

Exemptions to Confidentiality

In certain circumstances personal information may be disclosed and guidance is below. However it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Manager/Senior Clinician or the Caldicott Guardian.

Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where the subject's right to confidentiality may be overridden are rare.

Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs
- Where there is a serious threat to the healthcare professional or other staff

- Where there is a serious threat to the community
- In other exceptional circumstances, based on professional consideration and Consultation.

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- Terminations - Abortion Regulations 1991
- Child abuse - Children's Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g. terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from a senior Clinician or Senior Manager, the Head of Information Governance, the SIRO or the Caldicott Guardian.

The Trust will support any member of staff, who after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

Non-Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party.

Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care or in the course of their employment. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed.

The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous. Further guidance is available in the Access to Personal Records Policy (Patient/Employee).

9.4 Personal Identifiable Data in Medical Research

All project based research within the Trust must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy, be registered by the Research and Development Department and undergo review through the NHS Health Research Authority (HRA) approval process to provide assurance to our Trust, our patients and the public that all research meets the necessary legal and compliance standards.

The legal basis for processing confidential data for health and social research is '**a task in the public interest'**; (6(1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'

The Research & Development Department will log and retain as appropriate, all relevant data protection agreements and HRA approvals for research studies, as evidence for compliance with the General Data Protection Regulation 2018.

6 Monitoring and Review

Minimum requirement to be monitored	Lead	Frequency of Report of Compliance	Reporting arrangements
DSPT	IG Manager	Quarterly	
Data Quality audit	Head of clinical assurance	Quarterly	
IG Breaches	IG Manager	Quarterly	
SAR responses	Head of Corporate Governance and Legal	Quarterly	

7 Training and Implementation

7.1 All staff are required to complete their annual Data Security and Protection training either on-line or through classroom based sessions. Bespoke training is also available upon request.

7.2 Compliance with this policy is monitored via:

- The percentage level of staff completing training

- Monthly management information on the level of subject access requests completed within the statutory deadline
- The level of data breach incidents reported via Datix
- The level of data breach incidents escalated to the ICO via the IG Toolkit

8 Equality Impact Assessment

All public bodies have a statutory duty under The Equality Act 2010 (Statutory Duties) Regulations 2011 to provide "evidence of analysis it undertook to establish whether its policies and practices would further, or had furthered, the aims set out in section 149(1) of the [Equality Act 2010]"; in effect to undertake equality impact assessments on all procedural documents and practices. Authors should use the Equality Impact Toolkit to assess the impact of the document.
In the first instance this will mean screening the document and, where the screening indicates, completing a full assessment. The Toolkit can be found on the Trust website http://www.medway.nhs.uk/our-foundation-trust/publications/equality-and-diversity/equality-impact-assessments/

A document will not be considered approved until the author has confirmed that the screening process has been carried out and where required a full impact assessment has been completed. Where a full assessment is completed this should be submitted along with the document for approval.

9 References

Document	Ref No
References:	
General Data Protection Regulations (GDPR) May 2018. This EU legislation provides controls on the handling of personal identifiable information for all living individuals. In Article 5 of the GDPR the principles of processing are listed along with the principle of accountability and the duty of data controllers to demonstrate compliance to the following: • Lawfulness, fairness and transparency • Purpose limitation – data is collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes • Data minimisation – data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed • Accuracy – every reasonable step must be taken to ensure that personal data is correct and up to date. Inaccurate data may need to be erased or rectified without delay • Storage limitation – data should be kept for no longer than necessary • Integrity and confidentiality – protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. **Data Protection Act (DPA) 2018**	

This UK Act supplements the GDPR and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply.

Access to Health Records Act 1990

This Act provides controls on the management and disclosure of health records for deceased persons. The personal representative of the deceased or a person who might have a claim arising from the patient's death can request access to the patient's data.

Common Law Duty of Confidentiality

Case law which prohibits the use and disclosure of information provided in confidence unless there is a statutory requirement or court order to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example to protect the vital interests of the data subject or another person or for the prevention or detection of a **serious** crime.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access.

The laws mentioned above are the main regulations which drive the data protection agenda. However there are many additional laws which may have an impact on data protection.

- Access to Medical Reports Act 1988
- Communications Act 2003
- Crime and Disorder Act 1998
- Data Retention (EC Directive) Regulations 2009
- Environmental Information Regulations (2004)
- Freedom of Information Act 2000
- Health and Social Care Act 2008
- Health and Social Care (National Data Guardian) Act 2018
- Human Rights Act 1998
- Mental Capacity Act 2005
- NHS Care Record Guarantee 2011
- Privacy and Electronic Communications Regulations 2003
- Public Records Act 1958
- Regulation of Investigative Powers Act 2000

NATIONAL GUIDANCE

Confidentiality: NHS Code of Practice 2003

This code provides detailed guidance for NHS bodies concerning confidentiality and patient's consent to use their health information. It also details the required practice the NHS must take concerning security, identifying the main legal responsibilities for an organization and also details employee's responsibilities.

Caldicott Reports

These reports provide guidance to the NHS on the use and protection of person identifiable data, and emphasizes the need for controls over the availability of such information and access to it. It makes a series of recommendations and identifies that all NHS organisations are to ensure that they have an appointed Caldicott Guardian who is responsible for compliance with the Caldicott Principles and Standards.

- Justify the purpose
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

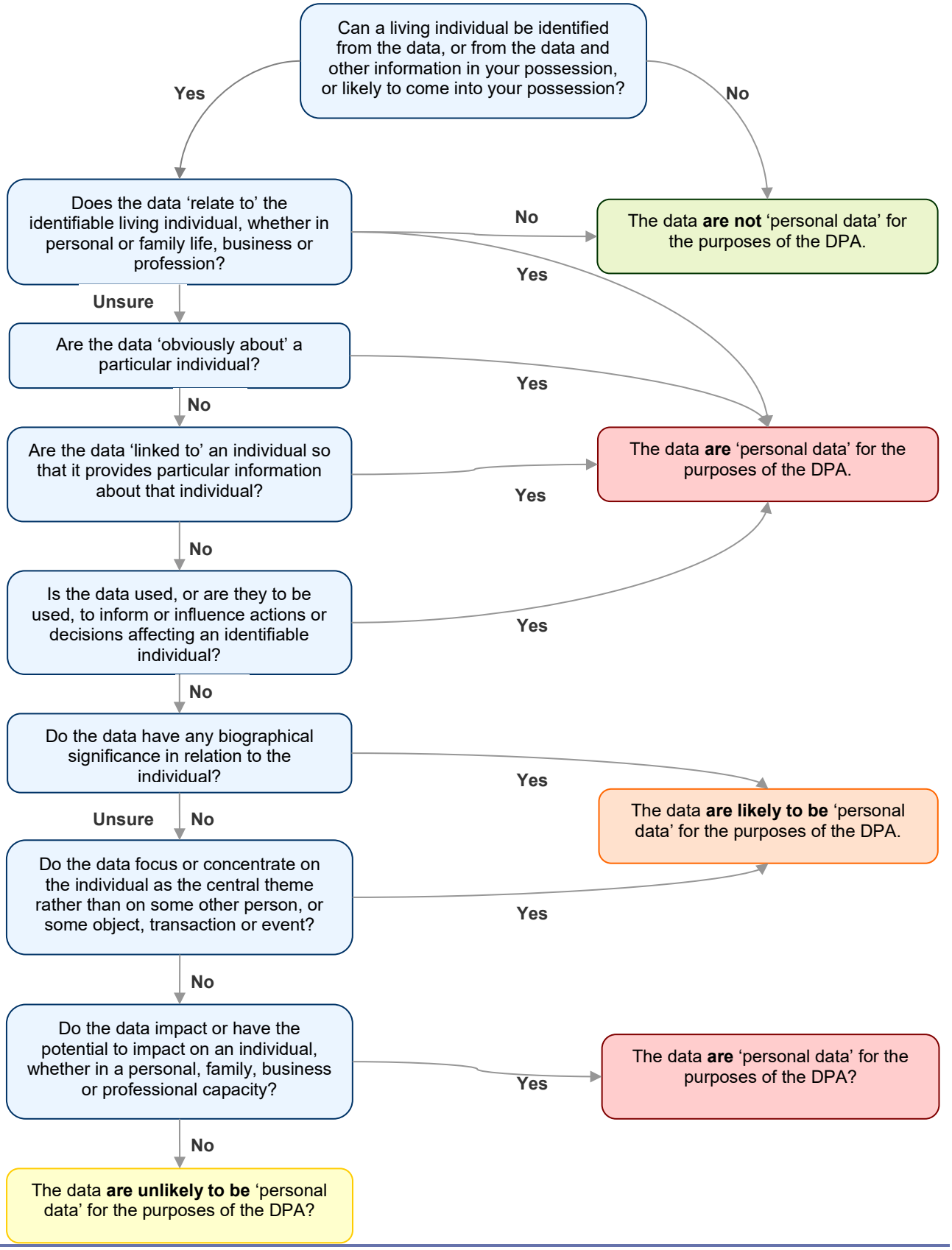
Additional guidance can be found in the following:

- CQC Safe data, safe care (2016)
- Data Retention (EC Directive) Regulations 2009
- Data Security Standards (2017)
- Data Security and Protection Requirements (2017)
- Information Security Management: NHS Code of Practice (2007)
- National Data Guardian for Health and Care Review of Data Security, Consent and Opt-outs (2016)
- NHS Constitution 2015
- Records Management Code of Practice for Health and Social Care 2016
- Review of Data Security, Consent and Opt-Outs NDG (2016)
- Safe data, safe care CQC (2016)
- The Employment Practices Code (ICO 2005)
- Your Data: Better security, better choice, better care DH (2017)

Trust Associated Documents:	
Information Security Policy	POLCGR018
Remote Access Policy	POLCGR084
Network Security Policy	POLCGR082
Acceptable Use of Trust Information Assets	POLCGR113
Secure Transfer of Information Policy	POLCGR077
Information Governance Policy	POLCGR017
Information Governance Strategy	STRCGR013

END OF DOCUMENT

Appendix 1 Personal Data Flow Chart



Appendix 2 Legal basis for processing

Processing Personal Data Article 6(1) GDPR

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Processing Special Category Data Article 9(2) GDPR

(a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.