University Hospital Southampton
NHS Foundation Trust

# Data Protection and Confidentiality Policy

| | | | |
|---|---|---|---|
| Trust reference | CA006 | Version number | 6.0 |
| Description | This policy and procedure inform how data protection and confidentiality is implemented throughout the Trust | | |
| Level and type of document | Level 1: applicable across the Trust<br>Trust-wide corporate policy – controlled document | | |
| Target audience | This policy is relevant to all staff, contractors, and members of the public | | |
| List related documents/policies (do not include those listed as appendices) | Records Management Policy<br>Incident Management Policy<br>Access to Records Policy<br>Informatics Security Policy<br>Management of Medical Devices Policy<br>Disciplinary Policy | | |
| Author | Judith Downing, Head of Data Protection | | |
| Policy sponsor | Karen Flaherty, Associate Director of Corporate Affairs | | |

This is a controlled document. Whilst this document may be printed, the electronic version posted on Staffnet is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from Staffnet.

## 1 Version control

| Date | Author(s) | Version created | Approval committee | Date of approval | Date next review due | Key changes made to document |
|---|---|---|---|---|---|---|
| July 2021 | Judith Downing | 6.0 | Quality Governance Steering Group | Chair's action 19.8.21 | 1 May 2022 | |
| | | | | | | |
| | | | | | | |

# 2 Index

# 3 Introduction

Data is central to the way the Trust enables effective treatment, supports world leading research, and plans its resources. Personal data (any information which can identity an individual) belonging to current, past, and prospective patients, employees, suppliers, contractors, and business partners is one of our most valuable assets in providing care.

This, together with the increasing reliance on IT to process and share information within the Trust environment, creates a greater need to protect data processed with the Trust's information systems and regulate access to external systems hosted on the internet and other remote locations.

The Data Protection Act 2018 and UK GDPR sets out the legal framework by which we can process personal information safely and securely, and operates alongside the common law duty of confidentiality which governs information given in confidence to health professionals with the expectation that it will be kept confidential

The UK GDPR sets out seven data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the seven data protection principles is unlawful.

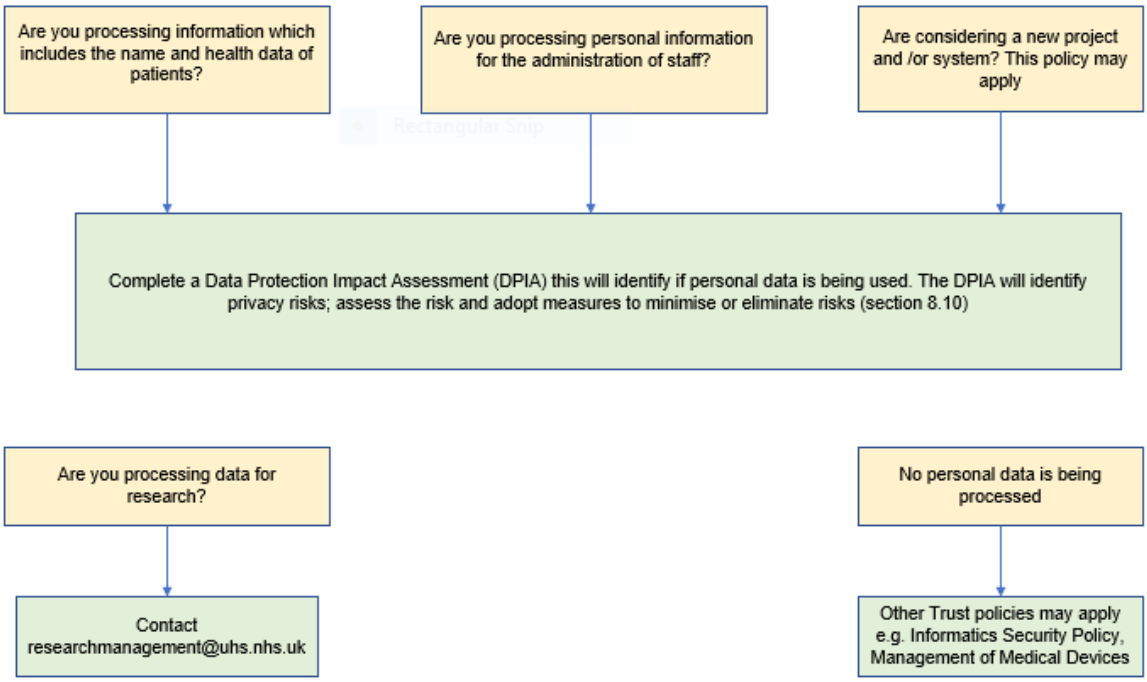
As a data controller we are responsible for ensuring compliance with the UK GDPR, and we must be able to demonstrate our compliance. To comply with the principles of UK GDPR the Trust must identify a lawful basis for processing, or the processing will be unlawful.

The Trust is required to register annually with the Information Commissioner's Office, which is the UK's independent body set up to uphold information rights. The Trust's unique registration number is **Z4989884.**

The Trust is also mandated by the Department of Health and Social Care (DHSC) to measure our performance against 10 data security standards set out by the National Data Guardian. The Data Security and Protection Toolkit (DSPT) is used to measure compliance.

Although the UK GDPR does not apply to deceased persons, the NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as to one who is alive. There is also separate legislation that applies when accessing health records of a deceased person, the Access to Health Records Act 1990. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought in the first instance from the data protection officer dataprotection@uhs.nhs.uk

# 4 Quick reference




# 5 Scope and purpose

This policy applies to all Trust staff, contractors and third parties who process personal data on behalf of the Trust to ensure that data is handled in accordance with the principles of the UK GDPR.

It will apply to all Trust and non-Trust employees who process personal data using information systems provided for them to perform their role within the organisation or who handle documentation on behalf of the Trust.

The policy will demonstrate the ways in which we ensure that the personal data of patients, employees, contractors, and business partners is handled effectively and securely.

The policy will promote best practice when processing personal data to inform care and research, and to ensure that Trust staff, contractors and third parties understand both the Trust's and their own personal responsibilities when handling personal data.

# 6 Definitions

| Term | Definition |
|---|---|
| Caldicott Guardian | A senior person within a health or social care organisation who makes sure that the personal information about those who use its services is used legally, ethically, and appropriately, and that confidentiality is maintained |
| Data Controller | An entity that decides how and why personal data is used e.g. the Trust |
| Data Processor | An entity that processes data for and on behalf of the Data Controller |
| Data Protection Act 2018 (DPA) | Sets out the data protection framework for the UK and replaces the Data Protection Act 1998 |

| | |
|---|---|
| Data Protection Impact Assessment (DPIA) | A process used within the Trust to identify and minimise the data protection risks of a project |
| Data Protection Officer (DPO) | The UK GDPR requires that a DPO is appointed by a public authority or body and organisations carrying out certain types of processing activities |
| Data protection by design and by default | Implementation of the data protection principles to put in place the appropriate technical and organisational measures and to safeguard individual's rights |
| Data Security and Protection Toolkit (DSPT) | A mandatory annual assessment by NHS Digital which measures our performance against the National Data Guardian's ten data security standards |
| Data subject | Someone who can be identified as a person, or with a combination of other information can be identified |
| Individual rights | There are eight rights for individuals, which have been strengthened in the UK GDPR. A data subject can ask us to do something or stop doing something with their personal data |
| Lawful basis | The reason or legal grounds we rely on to use people's personal data. There are six bases to choose from |
| National Data Guardian | Advises and challenges the health and care system to ensure individual confidential information is safeguarded securely and used properly |
| Personal data | Any information, which directly or indirectly can identify an individual such as name, identification number or contact details |
| Processing | Any action taken with someone's personal data e.g. collecting, recording, organising, sharing, erasure or destruction. |
| Pseudonymisation | The processing of personal data in a way that it cannot be attributed to a specific data subject without the use of additional information, provided that additional information is kept separate |
| Senior Information Risk Owner (SIRO) | An executive director or member of the board of directors with overall responsibility for an organisation's information risks |
| Special category data | Personal data which requires additional protections |
| UK GDPR | Is the retained version of the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales |

# 7 Key principles

The DPA and the UK GDPR set out the legal requirements and duties placed on data controllers (the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about).

The policy will inform you how the UK GDPR applies to the Trust and our obligations.

Under the UK GDPR each controller of personal information must decide what the lawful basis is for processing personal information. If there is no relevant basis, then the processing is likely to be illegal and regulatory action could be taken against the Trust.

# 8 Key principles of data protection

## 8.1 UK GDPR principles

The UK GDPR has seven key principles which set out how the Trust must process personal data. Compliance against the principles is a key and failure to comply may lead to regulatory action against the Trust.

The principles are:

| | |
|---|---|
| **Lawfulness, fairness, and transparency** | Processing has to be lawful and handled in a way which patients/staff would reasonably expect. We must be clear how we process personal data |
| **Purpose limitation** | The Trust must be clear on the purpose of processing<br>The Trust needs to record the purpose of processing |
| **Data minimisation** | Data must be adequate – sufficient to fulfil the purpose<br>Relevant – linked to the purpose<br>Limited – do not hold more than you need for that purpose |
| **Accuracy** | Take reasonable steps to ensure personal data is not incorrect or factually misleading |
| **Storage limitation** | Personal data must not be kept longer than necessary for the purpose for which it was processed |
| **Integrity and confidentiality (security)** | We must ensure the appropriate technical and organisational measures are in place |
| **Accountability** | We are responsible for complying with the UK GDPR and must demonstrate our compliance |

Each principle is detailed in appendix 1

### 8.2 Lawful basis for processing

The Trust is obligated to have lawful basis to process personal data. There are six lawful bases for processing, a lawful basis must be determined before processing begins.

The Trust also processes special category information, which requires more protection. In order to lawfully process special category data we need to identity a condition for processing, this is in addition to the lawful basis (Article 6 of the UK GDPR). This is known as an Article 9 condition.

Each lawful basis is detailed in appendix 2

### 8.3 Caldicott principles

The Caldicott principles focus on the protection and processing of patient identifiable information within the NHS. These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

The principles below are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and which they would reasonably expect to be kept private. This may include for instance, details about symptoms, diagnosis, treatment, names, and addresses.

| | |
|---|---|
| **Principle 1** | Justify the purpose(s) for using confidential information |
| **Principle 2** | Use confidential information only when it is necessary |
| **Principle 3** | Use the minimum necessary confidential information |
| **Principle 4** | Access to confidential information should be on a strict need-to-know basis |
| **Principle 5** | Everyone with access to confidential information should be aware of their responsibilities |
| **Principle 6** | Comply with the law |
| **Principle 7** | The duty to share information for individual care is as important as the duty to protect patient confidentiality |
| **Principle 8** | Inform patients and service users about how their confidential information is used |

The Trust appointed Caldicott Guardian (Chief Nursing Officer) advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Trust's Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures.

Full details of the principles can be found at appendix 3.

### 8.4 Duty of confidentially

A duty of confidentiality is when one person discloses information to another e.g. patient to clinician in circumstances where it is reasonable to expect that information will be held in confidence. It is:

- A legal obligation derived from case law
- A requirement established within professional codes of conduct
- Included in all NHS staff members' contracts of employment.

Patients entrust staff with information about their health and treatment. They do so in confidence and have an expectation that staff will respect their privacy.

It is essential that the Trust is seen to provide a confidential service to patients and breaches of that confidentiality may lead to regulatory investigation and can result in disciplinary measures to those who have been negligent in causing the breach (see section 8.12).

### 8.5 Data Processing

Data processing covers the collecting, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintain confidence between the Trust and its patients, staff, and others with whom we work.

The UK GDPR requires that processing of any personal information held by the Trust must comply with principles and has a lawful basis.

Routine data processing for the purposes of patient care will normally be conducted for a purpose that satisfies one of the processing conditions in the UK GDPR. When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

By complying with data protection legislation the Trust is also likely to comply with the provisions of Article 8 of the Human Rights Act 1998 (right to respect for their private and family life, home, and correspondence) in relation to the sharing of personal data.

### 8.6 IT systems

It is essential that IT systems holding personal data have adequate controls in place to prevent loss, unlawful processing, or inappropriate access.

The Informatics Security Policy provides detailed guidance on the security of Trust IT systems including minimum standards of access controls.

Staff should not attempt to access or use electronic record systems they have not been trained to use or authorised to access. Existing system users should not allow others to access systems using their login credentials.

Sharing system passwords is a disciplinary offence and viewed as a serious breach of Trust procedure.

## 8.7 Communicating personal information

In order to provide effective care services there is a need to transfer information between organisations and individuals. In order to comply with the UK GDPR principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any data containing identifiable information transferred by the Trust outside the Trust for processing must be securely encrypted during transit. Detailed guidance can be found in the Informatics Security Policy.

## 8.8 Access to information

**Staff**

Access to personal information is restricted and staff are prohibited from accessing or using patient information where there is no justification to do so.

While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is prohibited and may be unlawful.

Staff have no right to access personal information held in records about their relatives or friends.

The Trust's digital clinical systems will allow a user to access any individual record held in that system. Users must only access individual personal records for those data subjects (patients, staff etc.) that they have authorisation to access for specific purposes.

The Trust carries out audits of access to personal data and any member of staff who is found to be in breach of this guidance by inappropriately accessing their own or other people's records or personal data may face disciplinary action (see section 8.12).

In the case of unauthorised access to the Trust's computer systems including hacking and/or improper use of duly authorised credentials and the subsequent use of that data may result in a criminal action under the terms Computer Misuse Act 1990.

**Individual Rights**

The UK GDPR provides enhanced rights for all individuals. These rights are mandated in the UK GDPR and the Trust is required to act within a specific timeframe to any information request made to the Trust.

There are eight rights which all Trust employees and non-employees are required to be familiar with the rights of individuals and follow the Access to Records policy.

The eight rights are:

| Information right | Meaning |
|---|---|
| **The right to be informed** | Individuals have the right to be informed about how their data is used, which is included in the Trust's privacy notice |
| **The right of access (Subject Access Request)** | Individuals have the right ask for and receive a copy of their personal data |
| **The right to rectification** | Individuals have the right to have inaccurate personal data rectified or completed if incomplete |
| **The right to erasure (Right to be forgotten)** | Individuals have the right to ask for information to be erased; this is not an absolute right |
| **The right to restrict processing** | Individuals have the right to request the restriction or suppression of their personal data; this is not an absolute right |
| **The right to data portability** | Allows individuals to obtain and reuse their personal data for their own purposes |
| **The right to object** | Individuals have the right to object to the processing of their personal data in certain circumstances |
| **Rights in relation to automated decision-making and profiling** | Where there is no human involvement in decision-making or profiling, this is restricted and can be challenged |

### 8.9 Data protection by design and by default

As part of the UK GDPR's accountability principle the Trust is required to safeguard individual rights by putting in place the appropriate technical and organisational measures. The UK GDPR requires the Trust to integrate data protection into every aspect of processing activity.

This includes implementation of the data protection principles and safeguarding individual rights, such as data minimisation, pseudonymisation and purpose limitation as set in this policy.

The Trust requires that data protection must be considered at the start of any new project, service, or process.

### 8.10 Data Protection Impact Assessment (DPIA)

A DPIA identifies and assesses potential risks to the Trust of processing activities. It is an integral part of data protection by design and by default, and should be completed for all projects, proposals or business changes that involve personal information.

A template DPIA can be obtained by contacting dataprotection@uhs.nhs.uk.

### 8.11 Data sharing – third parties

Where the Trust, as Data Controller, instructs a third-party organisation to process data on their behalf there is a requirement to ensure the processor provides "sufficient guarantees" that they have the appropriate technical and organisational measures in place to ensure the processing complies with the UK GDPR and protects the rights of individuals.

### 8.12 Breach of data protection and confidentiality

Any breach or suspected breach of data protection and confidentiality can have severe implications for the Trust, our patients, and staff. Where significant numbers of patients are involved, this can impact on the reputation of the NHS as a whole.

The Trust is required to report serious breaches within 72 hours of the being made aware of the breach (where possible). The DPO is the single point of contact for all breaches and advice and guidance must be sought as soon as possible by contacting dataprotection@uhs.nhs.uk.

Staff must who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Incident Management Policy.

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA and UK GDPR constitutes a serious disciplinary offence or gross misconduct under the Trust's Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

### 8.13 Disposal of personal information

It is a principle of the UK GDPR that data should 'not be kept for longer than necessary'. To assist staff in meeting this requirement the Trust's Records Management Policy provides detailed guidance to staff about the minimum retention periods applicable to Trust records and record disposal procedures.

The Trust reports a significant number of incidents relating to the inappropriate disposal of manual records. All printouts, reports and printed copies of records containing personal data should be kept securely at all times; this includes but is not limited to handover reports and documents used by staff working in ward areas.

Any documents containing personal data should be disposed of securely and not discarded in general waste or recycling bins. The Trust waste management team operates a confidential waste disposal service and provides regular collections of confidential waste from all Trust areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops, and any other devices with information storage capabilities) should be carried out through the Informatics department to ensure all data is effectively removed before disposal.

The disposal of medical devices and equipment should follow the guidance on decommissioning and disposal provided in the Trust's Management of Medical Devices Policy.

## 9 Roles and responsibilities

**Chief Executive**

As the accountable officer the Chief Executive Officer is responsible for overall leadership and management of the Trust and has the ultimate responsibility for ensuring compliance with the Data Protection Act 2018, UK GDPR, Human Rights Act 1998, and the common law duty of confidentiality. The Chief Executive Officer delegates aspects of their responsibility to relevant executive directors according to their organisation portfolios.

**Caldicott Guardian**

The Trust has appointed the Chief Nursing Officer as the Trust's Caldicott Guardian. They are responsible for protecting the confidentiality of patient and service user information while enabling appropriate information sharing.

**Senior Information Risk Owner (SIRO)**

The Trust has appointed the Chief Operating Officer as the SIRO. They are responsible for information risk and to ensure that effective systems and processes are in place to address the

Trust's information governance agenda.

**Data Protection Officer (DPO)**
The Head of Data Protection, FOI and Disclosures is the Trust's DPO with responsibility for ensuring the Trust complies with data protection legislation and for its compliance with its own policies in relation to the protection of personal data.

The day-to-day responsibility for data protection and confidentiality falls within the remit of the DPO.

**Divisional and Care Group/Departmental Managers**
Managers are responsible for the local implementation of this policy in their areas of responsibility.

**Individual responsibility**
Everyone working for the NHS has a legal duty to keep information about patients and other individuals such as carers, relatives, staff, or volunteers confidential. They are required to adhere to confidentiality agreements i.e. common law duty of confidentiality, contract of employment, NHS confidentiality code of practice.

The terms and conditions within Trust employment contracts include specific conditions relating to data protection and confidentiality.

## 10 Communication and training plans

This data protection and confidentiality policy will be made available on Staffnet and awareness cascaded through divisional governance group meetings.

All staff are required to undertake mandatory induction and mandatory annual refresher training by using the virtual learning environment (VLE) module. This requirement applies to agency staff and contractors working at the Trust who may have access to personal information. Most agencies working with the NHS provide their staff with this training. Where this not the case local arrangements should be made to ensure the employee is adequately trained before working at the Trust.

## 11 Equality impact assessment

Equality and diversity are at the heart of Trust values. Throughout the development of the policies we give regard to the need to eliminate discrimination, harassment, and victimisation, to advance equality or opportunity, and to foster good relations between people who share a relevant protected characteristic (as cited in under the Equality Act 2010) and those who do not share it.

As part of its development this data protection and confidentiality policy and its impact on equality has been analysed and no detriment has been identified. The requirements relating to special category data afford additional protection in relation to some protected characteristics.

The Policy & Guidance Team hold all equality impact assessments centrally. These are available upon request from Policy&Guidance@uhs.nhs.uk

## 12 Document review

All Trust policies will be subject to a specific minimum review period of one year; we do not expect policies to be reviewed more frequently than annually unless changes in legislation occur or new evidence becomes available. The maximum review period for policies is every three years. The author of the policy will decide an appropriate frequency of review between these boundaries.

Where a policy becomes subject to a partial review due to legislative or national guidance, but the majority of the content remains unchanged, the whole document will still need to be taken through the agreed process as described in this policy with highlighted changes.

This Data Protection and Confidentiality Policy will be reviewed in May 2022.

## 13 Process for monitoring compliance

The purpose of monitoring is to provide assurance that the agreed approach is being followed. This ensures that we get things right for patients, use resources well and protect our reputation. Our monitoring will therefore be proportionate, achievable and deal with specifics that can be assessed or measured.

Key aspects of this policy will be monitored:

| | |
|---|---|
| Element to be monitored | Compliance with Data Protection and Confidentiality Policy |
| Lead (name/job title) | Head of Data Protection |
| Tool | Incidents reported relating to data protection and confidentiality |
| Frequency | Quarterly |
| Reporting arrangements | Quality Governance Steering Group |

| | |
|---|---|
| Element to be monitored | Compliance with Data Protection and Confidentiality Policy |
| Lead (name/job title) | Head of Data Protection |
| Tool | Personal data breaches reported to Information Commissioner's Office |
| Frequency | Annual |
| Reporting arrangements | Annual report |

| | |
|---|---|
| Element to be monitored | Staff training |
| Lead (name/job title) | Head of Data Protection |
| Tool | Compliance levels with induction and annual mandatory information governance training |
| Frequency | Annual |
| Reporting arrangements | Quality Governance Steering Group |

| | |
|---|---|
| Element to be monitored | Individual rights |
| Lead (name/job title) | Head of Data Protection |
| Tool | Subject access requests received and responded to with statutory response time |
| Frequency | Quarterly |
| Reporting arrangements | Audit and Risk Committee |

| | |
|---|---|
| Element to be monitored | Data protection by design and by default |
| Lead (name/job title) | Head of Data Protection |
| Tool | Number of data protection impact assessments (DPIA) completed |
| Frequency | Quarterly |
| Reporting arrangements | Audit and Risk Committee |

Where monitoring identifies deficiencies actions plans will be developed to address them.

## 14 Appendices

Appendix 1: UK GDPR – Principles
Appendix 2: UK GDPR – Lawful bases, conditions, and special category data
Appendix 3: Caldicott Principles

## 15 References

Data Protection Act 2018
UK General Data Protection Regulation
Access to Health Records Act 1990
Human Rights Act 1998
Information Commissioner's Office website
The Caldicott Principles and associated guidance from the National Data Guardian
Department of Health Confidentiality: NHS Code of Practice (November 2003)

## Appendix 1: UK GDPR – Principles

| The UK GDPR sets out seven key principles with which the Trust is required to comply | |
|---|---|
| **Article 5(1)(a) Lawfulness, fairness and transparency** | Personal data shall be:<br><br>(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency') |
| **Article 5(1)(b) Purpose limitation** | Personal data shall be:<br><br>(b) 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 |
| **Article 5(1)(c) Data minimisation** | Personal data shall be:<br><br>(c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation') |
| **Article 5(1)(d) Accuracy** | Personal data shall be:<br><br>(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') |
| **Article 5(1)(e) Storage limitation** | Personal data shall be:<br><br>(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 subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation') |
| **Article 5(1)(f) Integrity and confidentiality (security)** | Personal data shall be:<br><br>(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 |
| **Article 5(2) Accountability** | The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability') |

## Appendix 2: UK GDPR – Lawful bases, conditions, and special category data

| The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the Trust processes personal data | |
|---|---|
| **Article 6(1)(a) Consent** | the individual has given clear consent for you to process their personal data for a specific purpose |
| **Article 6(1)(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 |
| **Article 6(1)(c) Legal obligation** | the processing is necessary for you to comply with the law (not including contractual obligations) |
| **Article 6(1)(d) Vital interests** | the processing is necessary to protect someone's life |
| **Article 6(1)(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 |
| **Article 6(1)(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.) |

| **Special category data includes Article 9(1)** |
|---|
| personal data revealing **racial or ethnic origin** |
| personal data revealing **political opinions** |
| personal data revealing **religious or philosophical beliefs** |
| personal data revealing **trade union membership** |
| **genetic data** |
| **biometric data** (where used for identification purposes) |
| data concerning **health** |
| data concerning a person's **sex life** |
| data concerning a person's **sexual orientation** |

| **If special category data is processed one of the following condition(s) must be also be met. Article 9 lists the conditions for processing special category data** | |
|---|---|
| **Article 9(2)(a) Explicit consent** | the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject |
| **Article 9(2)(b) Employment, social security and social protection (if authorised by law)** | 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 domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject |
| **Article 9(2)(c) Vital interests** | 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 |
| **Article 9(2)(d) Not-for-profit bodies** | 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 |
| **Article 9(2)(e)<br>Made public by the data subject** | processing relates to personal data which are manifestly made public by the data subject |
| **Article 9(2)(f)<br>Legal claims or judicial acts** | processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity |
| **Article 9(2)(g)<br>Reasons of substantial public interest (with a basis in law)** | processing is necessary for reasons of substantial public interest, on the basis of domestic 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 |
| **Article 9(2)(h)<br>Health or social care (with a basis in law)** | 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 domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 (processed by or on behalf of a professional subject to professional secrecy obligation) |
| **Article 9(2)(i)<br>Public health (with a basis in law)** | 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 domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy |
| **Article 9(2 (j)<br>Archiving, research and statistics (with a basis in law)** | processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the DPA) based on domestic 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 |

## Appendix 3: Caldicott Principles

| | |
|---|---|
| **Principle 1: Justify the purpose(s) for using confidential information** | Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian. |
| **Principle 2: Use confidential information only when it is necessary** | Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible. |
| **Principle 3: Use the minimum necessary confidential information** | Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function. |
| **Principle 4: Access to confidential information should be on a strict need-to-know basis** | Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes. |
| **Principle 5: Everyone with access to confidential information should be aware of their responsibilities** | Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users. |
| **Principle 6: Comply with the law** | Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law. |
| **Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality** | Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies. |
| **Principle 8: Inform patients and service users about how their confidential information is used** | A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required. |