Gloucestershire Hospitals
NHS Foundation Trust

# TRUST POLICY

# DATA PROTECTION AND CONFIDENTIALITY

**This document may be made available to the public and persons outside of the Trust as part of the Trust's compliance with the Freedom of Information Act 2000.**

**Please be aware that only documents downloaded or viewed directly from the GHNHST Trust Policies webpage are valid documents. Documents obtained through printed copies or internet searches may be out of date and therefore will be invalid.**

**In this document you may find links to external websites. Although we make every effort to ensure these links are accurate, up to date and relevant, Gloucester Hospitals NHS Trust cannot take responsibility for pages maintained by external providers.**

**FOR USE BY:**
**This Policy is to be followed by all staff of Gloucestershire Hospitals NHS Trust and Gloucestershire Managed Services (GMS)**

**FAST FIND:**

- B0745 - Guidance on the Serious Harm Test
- Information Governance Policy
- IT Security Policy
- Records Management Policy
- Clinical Records Keeping Standards
- Access to Information Systems by Persons not Employed by the Trust Procedure

## 1. INTRODUCTION / RATIONALE

This policy provides the framework to ensure that the Trust complies with the requirements of statutory and legal frameworks relating to the use of Personal Confidential Data, including:

- Data Protection Act 2018
- The UK GDPR
- Human Rights Act 1998
- The common law duty of confidentiality
- Caldicott Principles
- NHS Code of Confidentiality
- Freedom of Information Act 2000

## 2. DEFINITIONS

| Word/Term | Descriptor |
|---|---|
| shall / must | These terms are used to state a Mandatory requirement of this policy |
| should | This term is used to state a Recommended requirement of this policy |
| may | This term is used to state an Optional requirement |
| UK GDPR | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as implemented by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, The Data Protection, Privacy and Electronic Communications (Amendments etc.)(EU Exit) Regulations 2020 and any subsequent amendments thereto |
| DPA | The Data Protection Act 2018 |
| Data | For the purposes of this policy data includes recorded information in any form or format, whether hard copy or electronic, and whether part of a formal information system or simply held transiently. |
| Personal Data | Personal Data is defined in the UK GDPR as any information relating to an identified or identifiable natural person. |
| Personal Confidential Data | Personal information about identified or identifiable individuals, which should be kept private or secret. This includes Personal Data as defined above, but is extended to include deceased as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'. |
| Processing | any operation or set of operations which is performed on Personal Data |
| Pseudonymisation | means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person; |
| Special Category Data | data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation |

## 3. POLICY STATEMENT

The policy provides a robust framework to ensure a consistent approach to both compliance and best practice for data protection and confidentiality across the whole organisation, and supports the duties set out in the NHS Constitution and the requirements of the NHS Confidentiality Code of Practice 2003. It applies to all Trust staff (including temporary and agency staff and volunteers). They must comply with this policy as a condition of their employment.

The policy also comprises the Trust's policy document as required by Paragraph 34 of Schedule 1 Part 4 of the DPA in relation to processing of Personal Data carried out in reliance on a condition in Part 1, 2 or 3 of that Schedule, in cases where a separate policy document has not been used (Template RD4). It covers compliance with the principles in Article 5 of the UK GDPR and the Trust's policies as regards the retention and erasure of Personal Data.

This policy supports the aims and standards set out in Section 5 of the Trust's Information Governance Policy. It covers all Personal Data and Personal Confidential Data created, processed and stored by the Trust including, but not limited to, that relating to patients and staff.

**A BREACH OF THIS POLICY MAY RESULT IN DISCIPLINARY ACTION.**

## 4. ROLES AND RESPONSIBILITIES

| Post/Group | Details |
|---|---|
| Data Protection Officer | As required by Article 37 UK GDPR including:<br>• to inform and advise the Trust and its employees of their obligations pursuant to the Data Protection Legislation<br>• to monitor compliance with the Data Protection Legislation<br>• to provide advice as regards data protection impact assessments and monitor their performance |
| Trust Board | • To approve the Trust's Policy in respect of Information Governance, taking into account legal and NHS requirements. This role may be delegated to an appropriate sub-committee or executive director.<br>• To receive reports at least annually on the Trust's Information Governance performance. |
| Trust Senior Information Risk Owner (SIRO) (Director of Clinical Strategy) | • Named Executive Director on the Board with responsibility for Information Governance.<br>• To undertake the role of Senior Information Risk Owner (SIRO) for the Trust<br>• Chair of the Trust Information Governance and Health Records Committee<br>• To appoint the Lead for Information Governance<br>• To appoint a trust lead for Data Protection and Freedom of Information |
| Caldicott Guardian (Medical Director) | • Named Executive Director with responsibility for Caldicott and is a member and vice chair of the Information Governance and Health Records Committee. |
| Lead for Information Governance (Information Governance and Health Records manager) | • Overseeing day to day Information Governance issues<br>• Developing and maintaining policies, standards, procedures and guidance<br>• Co-ordinating Information Governance in the Trust and raising awareness of Information Governance<br>• Co-ordination of the completion and annual submission of the DSPT<br>• Lead on management of Information Governance Serious Incidents requiring<br>• investigation (IG SIRI) |
| The Information Governance and Health Records Committee | • Accountable to the Trust Leadership Team via the Chair<br>• Approving the results of information governance audits prior to presentation by the Trust Board |
| Managers | • To ensure that this Policy and any supporting documents are built into local processes<br>• To ensure that the development of any new systems will be compliant with Data Protection and Confidentiality requirements |
| All staff | • To ensure that they are aware of Data Protection and Confidentiality requirements and standards including responsibilities in relation to their specific role and are compliant with these standards and responsibilities<br>• To ensure that they complete IG and Code of Confidentiality mandatory training<br>• To report Data Protection and Confidentiality related incidents including data breaches through the trust incident reporting tool Datix<br>• To escalate any Data Protection and Confidentiality related concerns through their Line management and / or to the IG Lead<br>• |

| | |
|---|---|
| Information Asset Owners (Heads of Department and budget holders) | • Overall responsibility for information assets in their own area, however funded.<br>• To ensure that effective system management responsibilities are defined and that known risks are scored, recorded and escalated according to the Trust's risk management procedures. |
| System Managers | • To ensure that all suppliers, whether providing new systems or developing legacy systems show evidence of compliance with Data Protection and Confidentiality by completion of the DSPT for Commercial Third Parties or providing equivalent assurance<br>• To submit Information Governance Systems forms when required<br>• To provide evidence of compliance with Data Protection and Confidentiality requirements when requested |

## 5. DATA PROTECTION

### 5.1 Data Protection Principles

The Trust and its staff (including temporary and agency) will at all times comply with the data protection principles set out in Article 5 of the UK GDPR. These principles specify (in summary) that Personal Data must be:

- processed fairly and lawfully and transparently (Principle1)
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Principle2)
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle3)
- accurate and up to date (Principle4)
- kept no longer than necessary (Principle 5)
- protected in appropriate ways from unauthorised use, loss or disclosure (Principle6)

### 5.2 Compliance – Principle 1 ('lawfulness, fairness and transparency')

The Trust has procedures and measures to ensure compliance with principle 1 including but not limited to:

- Maintaining Privacy Notices (available on the Trust public website for patients) for all types of data processed which are kept up to date, made available to data subjects, and comply with the requirements of the UK GDPR and any Code of Practice issued by the Information Commissioner's Office (ICO)
- Appointing a Data Protection Officer, whose contact details are available to the data subjects
- Complying with the common law duty of confidentiality;
- Ensuring that the lawful basis for the processing of information is identified and included in Privacy Notices
- Ensuring that, where processing is by consent, such consent is freely given, specific, informed and unambiguous and obtained via a statement or by a clear affirmative action and in the case of Special Category Data such consent is explicit
- Ensuring that Personal Data is not informally shared with or disclosed to any third party. Any such sharing or disclosure will be controlled and appropriately authorised, will only be done where it is lawful to do so and notified to data subjects (if consent has not been obtained) unless UK GDPR or DPA provide an exemption and there is good and lawful reason to apply that exemption. When sharing Personal Data, the Trust will comply with any Code of Practice issued by the ICO

For patients the Trust identifies that in most cases Personal Data is processed in exercise of its official authority under various statutory duties including the requirement to maintain securely an accurate, complete and contemporaneous record in respect of each service user under Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Article 6(1)(e) UK GDPR).

In so far as patient records comprise Special Category Data the legal basis is typically that processing is necessary for the purposes of preventive or occupational medicine, or the provision of health or social care or treatment or the management of health or social care systems. (Article 9(2)(h) UK GDPR).

### 5.3 Compliance – Principle 2 ('purpose limitation')

The Trust has procedures and measures to ensure compliance with principle 2 including but not limited to:

- Maintenance of an Information Asset Register (IAR). The IAR will record the lawful basis for processing of the assets and the controls over any related data flows including information sharing and processing arrangements. The Trust IAR system is Flowz.
- Completion of Data Protection Impact Assessments for high-risk processing.

### 5.4 Compliance – Principle 3 ('data minimisation')

The Trust has procedures and measures to ensure compliance with principle 3 including but not limited to:

- Conducting routine audits as part of good data management practice.
- Ensuring that relevant records policies and professional guidelines are adhered to including appropriate Clinical Record keeping standards
- Ensuring that all processing of Personal Data is kept to the minimum necessary for compliance with the Trust's work and purposes and access to any Personal Data is restricted to those who need it for their work
- Ensuring that, where possible without interfering with the Trust's necessary work, or that of any third party with whom data is shared or to whom data is disclosed, any Personal Data is anonymised or pseudonymised before being used, shared or disclosed. The Trust will comply with the Information Commissioner's Anonymisation Code of Practice and NHS Guidance
- Maintaining registers of data sharing and data processing agreements with third parties. Data processing agreements will conform to the requirements of Articles 28 to 32 UK GDPR, be in writing, and impose equivalent responsibilities on any data processor to those set out in this policy.

### 5.5 Compliance – Principle 4 ('accuracy')

The Trust has procedures and measures to ensure compliance with principle 4 including but not limited to:

- Ensuring that data users record information accurately and take reasonable steps to check the accuracy of information they receive from data subjects or anyone else
- Conducting routine audits as part of good data quality management practice
- Providing guidance to staff on good records management practices including guidance on Clinical Record keeping standards
- Advising data subjects of their right to seek rectification and ensuring requests are acted upon as required.

### 5.6 Compliance – Principle 5 ('storage limitation')

The Trust has procedures and measures to ensure compliance with principle 5 including but not limited to:

- Maintaining and regularly reviewing a Records Management Policy or policies and procedures covering the creation, management and secure disposal of corporate, staff and patient records
- Ensuring that data users regularly check systems to destroy out-of-date information and correct inaccurate information.
- Compliance with the Department of Health's Records Management: NHS Code of Practice.

### 5.7 Compliance – Principle 6 ('integrity and confidentiality')

The Trust has procedures and measures to ensure compliance with principle 6 including but not limited to:

- Maintaining and regularly reviewing an IT Security Policy and associated procedures
- Maintaining and regularly reviewing a Policy and associated procedures for investigating and managing breaches or suspected breaches of data protection, confidentiality and/ or information security
- Completion of Data Protection Impact Assessments (DPIA) for new and changing high risk processes which handle Personal Data
- Ensuring that data protection by design and by default is built into its processes, in particular in relation to commissioning new information assets, new methods of processing and the use of new technology.
- Applying appropriate controls where third-party access is granted to Trust information systems in accordance with the Access to Information Systems by Persons not Employed by the Trust Procedure
- Complying with NHS and Government Security Management Standards including cyber security
- Ensuring that all Information Assets are owned and managed and risk assessments of those assets and associated information flows are undertaken and reviewed at appropriate intervals
- Maintaining a program of data protection, security and confidentiality audits
- Ensuring that appropriate guidance and training is available to staff on the steps they must take to comply with this policy
- Complying with the National Data Guardian's (NDG) Data Security Standards and completing annually the NHS Data Security and Protection Toolkit as evidence of compliance
- Ensuring that appropriate safe haven and faxing procedures are maintained for the transmission of personal data
- Ensuring that any transfer of Personal Data outside of the UK is compliant with Articles 44-49 of UK GDPR. Such transfers will not be made without consultation with the Trust's Data Protection Officer and in the case of confidential patient data without the approval of the Trust's Caldicott Guardian. Approvals and consultation may relate to regular or individual transfers.

### 5.8 Accountability and Records of Processing Activity

The Trust will complete a Data Protection Impact Assessment (DPIA) Screening for all new, or substantially changed activities which process personal data (RD2). Where indicated (processing which would be high risk in the absence of mitigation) a full DPIA will be conducted (RD3).

Where the lawful basis for processing personal data is identified as 'legitimate interest' a formal Legitimate Interest Assessment will be conducted (RD5)

The Trust will keep records of processing activities (ROPA) as required by Article 30 UK GDPR. The principle ROPA will be held in the Flowz Information Asset Register supplemented by this policy, the IT Security Policy (Art 30(1)(g)), the Records Management Policy and Retention Schedule (Art 30(1)(f)), and registers of Data Processing and Information Sharing Agreements together with the relevant agreements in force from time to time. ROPA may also be found in completed DPIAs including screenings which did not lead to a full DPIA. Where there is a new personal data flow with

an external controller without an Information Sharing Agreement a ROPA form RD7 must be completed.

The controller for all patient personal data is the Trust. The Trust and GMS are controllers for their respective employees' personal data. The Trust and GMS are joint controllers for the management of CCTV systems. The Trust's Associate Chief Information Officer IG and Health Records is Data Protection Officer for both organisations.

## 6. SUBJECT RIGHTS

Data subjects will be given straightforward procedures to enable them to exercise their rights set out below. Subject access procedures will be made available on the Trust website. The Trust will seek to comply with the statutory time limits for subject access requests.

The Trust will comply with the Information Commissioner's Subject Access Code of Practice and the NHS Care Records Guarantee. The Trust will where appropriate take into account the Information Commissioners Office (ICO) guidance on Access to Information in Complaints Files, and in relation to subject access requests by employees the ICO Employment Practices Code and Supplementary Guidance.

The Trust will maintain appropriate procedures and guidance for both staff and those interacting with the Trust to ensure that individuals are given and can exercise their rights under UK GDPR including:

- The right to information about the processing of their Personal Data under Articles 13 and 14 of UK GDPR in the form of privacy notices on the Trust website and in contracts, information leaflets, and explanations in correspondence where appropriate;
- The right of access to their Personal Data under Article 15 of UK GDPR;
- The rights of rectification, erasure and to restrict processing under Articles 16-18 of UK GDPR;
- The right to object to processing under Article 21 UK GDPR and to limit automated individual decision making and profiling under Article 22.

Where a data subject seeks to exercise a right of access to personal data please refer to AC2. For other rights see AC1. Where a patient seeks access to Health Records an appropriate Health Professional may need to consider the statutory "Serious Harm" test. See B0745 - Guidance on the Serious Harm Test.

## 7. CONFIDENTIALITY

### 7.1 Principles

The Trust and its staff shall at all times comply with the law of confidentiality, the requirements of the UK GDPR and DPA and the Human Rights Act 1998 so far as they affect confidentiality obligations and with the eight Caldicott principles which specify that the Trust should:

1. Justify the purpose(s) for using personal confidential data.
2. Only use it when absolutely necessary.
3. Use the minimum that is required.
4. Ensure that access is on a strict need-to-know basis.
5. Ensure that everyone understands his or her responsibilities.
6. Ensure that everyone understands and complies with the law.
7. Recognise that the duty to share information can be as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used.

The Trust adopts and expects all staff to abide by the principles in the 'Confidentiality: NHS Code of Practice' published by the Department of Health in 2003.

This document:

- introduces the concept of confidentiality;
- describes what a confidential service should look like;
- provides a high-level description of the main legal requirements;
- lists examples of particular information disclosure scenarios.

A summary of the key confidentiality issues can be gained by reading the main body of the document (pages 1-12). The supporting Annexes provide detailed advice and guidance on the delivery of a confidential service. It is supported by "Supplementary Guidance: Public Interest Disclosures" published in November 2010 which provides guidance to NHS staff in making what are often difficult decisions on whether a breach of patient confidentiality can be justified in the public interest.

## 7.2 Patient Confidentiality

In March 2013, the Health & Social Care Information Centre published "A guide to confidentiality in health and social care" which identified five rules for handling Personal Confidential Data about patients which encompass the Caldicott Principles. The Trust adopts and expects all staff to abide by those Rules:

**Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully.**

All staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

Confidential information must not be disclosed to third parties without prior discussion and confirmation with a senior manager in the Trust.

Staff should not access patient or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is considered to be within their role in the organisation.

Confidentiality clauses will be included in contracts of employment and engagement. Confidentiality clause will be included in contracts with 3rd party contractors and suppliers who process Personal Confidential Data.

**Rule 2: Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.**

The Trust and its staff will share information likely to facilitate the provision of health services or adult social care in the individual's best interests as required by S251B of the Health and Social Care Act 2015 providing this does not breach patient confidentiality.

Sharing arrangements will be notified to patients through the Trust's Privacy Notice and will be routinely discussed with patients at point of contact whenever possible and appropriate. Where this is done consent to share may be implied for the purposes of direct care.

Sharing within care pathways should be restricted to what is relevant necessary and proportionate.

Sharing Personal Confidential Data without consent may be possible without breaching confidentiality as set out in Section 7.4

See Action Card AC5 – Information Sharing

**Rule 3: Information that is shared for the benefit of the community should be anonymised**

Anonymised information may be shared for the benefit of the community including research and the management of health services. The Trust will apply the HSCIC Anonymisation Standard and have regard to any Code of Practice Issued by the ICO.

Patient Personal Confidential Data which has not been anonymised or de-identified will not be used for purposes other than direct care unless:

- the Trust has fully informed explicit consent
- there is a legal obligation to do so – see section 7.4
- the law allows sharing for a particular reason where there is overriding public interest e.g. control of infectious diseases or where regulations and legislation allow under s251 of the NHS Act 2006 – again see section 7.4

**Rule 4: An individual's right to object to the sharing of confidential information about them should be respected**

Where a patient objects to a disclosure, they should receive an explanation of the likely consequences of their decision but if it is maintained the objection must be respected except in exceptional circumstances - see section7.4 for examples. An explanation should be provided to the individual.

When considering an objection, the Trust will take into account:

- whether not supporting the objection will damage the effectiveness of care;
- whether there is a demonstrable risk that the safety of the patient will be reduced by not upholding the objection; and
- whether there are compelling legitimate grounds relating to the individual's situation.

**Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.**

This policy and associated documents and procedures are in compliance with Rule 5. Staff must report via Datix any incident or suspected incident in which security or confidentiality has or may have been breached in accordance with the Trust's Incident Management Policy.

All staff will be required to sign a Confidentiality Code of Conduct which adopts these rules. Staff should not access any information relating to themselves, in Trust records, including Health and Employee records unless they are directly involved in the patient/client's clinical care or with the employee's administration on behalf of the Trust.

The Trust will ensure that all organisations it shares confidential information with are committed to following the rules of confidentiality.

### 7.3 Patient Records

On admission and/or on first contact with the service for a particular matter, all patients should be asked which relatives, friends or carers they wish to receive information regarding treatment and progress, and those they specifically do not give permission to receive information. This information must be recorded in the clinical records or on TrakCare.

In cases where relatives have been heavily involved in patient care, the patient must be explicitly asked as to what level these relatives can be kept informed. This is particularly important in cases where relatives are requesting information on the patient's condition, perhaps before the patient has been informed.

As an active research organisation, Trust staff may screen patients' records to identify any potential research participants with the Consultant's permission. Patients may also be approached by staff regarding participation in a particular research study in order to obtain consent.

In the event of a patient being incapable of giving permission for any information sharing or use where required the Mental Capacity Act 2005 must be followed. Staff should refer to the Mental Capacity Act Policy and procedures for detail.

Health Professionals should also adhere to any guidance and standards of confidentiality published by their professional body. Key references are included in Section 10.

### 7.4 Disclosing Information against a patient's wishes

In certain circumstances personal information may need to be disclosed without consent or even despite objections. In such cases staff must 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 or Information Governance.

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.

When considering overriding confidentiality staff should follow AC3 Overriding Confidentiality.

Where appropriate the Trust's Safeguarding Policies must be followed.

In making decisions on disclosure without consent for non-care purposes the Trust will apply the National Data Opt-Out where required

The following are examples where disclosure is required by law and no 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. Section 47 of the Children Act 1989 imposes a legal obligation to supply information to a Local Authority exercising its child protection powers unless it would be unreasonable to do so.
- Section 45 of the Care Act 2014 imposes a legal obligation to disclose to a Safeguarding Adults Board if certain conditions are met.
- 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
- Section 8 of the National Audit Act 1983 imposes a legal obligation on public bodies to provide relevant information to the National Audit Office.
- S5B Female Genital Mutilation Act 2003
- Section 251 of the NHS Act 2006 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes where it is not possible to use anonymised information and where seeking consent is not practical, having regard to the cost and technology available. S251 Approvals will be subject to the National Data Opt-Out in most cases.

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

## 8. TRAINING

Training on confidentiality will be included within induction procedures for new staff and within the mandatory annual Information Governance refresher training for all staff.

The Trust will maintain a training needs analysis and provide appropriate training for staff with specialist roles including the Caldicott Guardian, SIRO, Information Governance team, and those handling information requests.

## 9. MONITORING OF COMPLIANCE

| | |
|---|---|
| Do the systems or processes in this document have to be monitored in line with national, regional or Trust requirements? | YES |

| Monitoring requirements and methodology | Frequency | Further actions |
|---|---|---|
| Monitoring Requirements as set out in the Trust's Information Governance Policy | See Information Governance Policy | See Information Governance Policy |

## 10. REFERENCES

**Although we make every effort to ensure these links are accurate, up to date and relevant, Gloucester Hospitals NHS Trust cannot take responsibility for pages maintained by external providers.**

General Medical Council: Confidentiality: good practice in handling patient information
General Medical Council: Making and using visual and audio recordings of patients
British Medical Association: Confidentiality and health records tool kit
Nursing and Midwifery Council: Code for nurses and midwives
Royal College of Radiologists: Guidance on maintaining patient confidentiality when using radiology department information systems, second edition
Royal College of Surgeons: Confidentiality and Disclosure of Health Information - Toolkit
Medical Defence Union: Safeguarding and Vulnerable Adults
Department of Health: Information Governance Review (Caldicott2)
NHS Digital: National Data Opt-Out Programme
Information Commissioner: Subject Access Code of Practice
Information Commissioner: Access to Information in Complaints Files

| DOCUMENT PROFILE | |
|---|---|
| Reference Number | B0734 |
| Title | Data Protection and Confidentiality |
| Category | Non-Clinical |
| Version | V2.1 (AMENDED SEPTEMBER 2023) |
| Issue Date | May 2022 |
| Review Date | May 2025 |
| Owning Division | Corporate |

| | |
|---|---|
| Owning Specialty | Information Governance |
| Associated Specialities | N/A |
| For Use By | GHNHST & GMS STAFF |
| Author | Phil Bradshaw, Information Governance & Data Protection Specialist |
| Quality Assurance Group | IGHR Operational Group<br>DCDG |
| Other Approving Groups | N/A |
| Local Approval Details | Information Governance and Health Records Committee (IGHR) 16 February 2022<br>DCDG Meeting 5th April 2022 |
| TPAG Ratification | May 2022 |
| Consultees | IM&T Leaders<br>IM&T Board |
| Dissemination Details | Upload to Policy Library, Policy Monthly Update<br>A copy of this Policy can be requested by the public as part of Trust Publication Scheme requirements and as a key component of Data Protection transparency requirements.<br>Any online privacy notices should provide a link to the policy. |
| Keywords | Information Governance, Data Protection, UK GDPR, Confidentiality, Caldicott, Freedom of Information, IG DSP Toolkit |
| Equality Impact Assessment (EIA) | B0734 EIA |
| Related Trust Documents | AC1 - Exercise of Subject Rights (Other Than Access)<br>AC2 - Exercise of Subject Access Rights<br>AC3 - Overriding the Duty of Confidentiality<br>AC4 - Redacting Documents<br>AC5 - Information Sharing<br>RD1 - Data Protection Impact Assessment Procedure<br>RD2 - Data Protection Impact Assessment Screening Template<br>RD3 - Data Protection Impact Assessment Template<br>RD4 - Policy Document Template<br>RD5 - Legitimate Interest Assessment<br>RD6 - Transfer Impact Assessment<br>RD7 - ROPA - Record of Processing Activity |
| Other Relevant Documents | B0745 - Guidance on the Serious Harm Test<br>B0413 - Information Governance Policy<br>B0591 - IT Security Policy<br>B0259 - Records Management Policy<br>B0218 - Clinical Records Keeping Standards<br>B0733 - Access to Information Systems by Persons not Employed by the Trust Procedure<br>B0393 - Incidents - Managing, Reporting and Reviewing of Incidents / Accidents, including Serious Incidents<br>B0291 - Disciplinary Procedure<br>Q0637 - Risk Management Strategy<br>B0636 - Risk Assessment / Risk Register Process<br>B0218 - Clinical Records Keeping Standards<br>Privacy Notice<br>Staff Privacy Notice |
| External Compliance Standards and/or Legislation | Department of Health: Confidentiality: NHS Code of Practice 2003 & Supplementary Guidance: Public Interest Disclosures<br><br>NHS Digital:<br>A guide to confidentiality in health and social care, 2013<br>Guide to Confidentiality reference document, 2013<br>Code of practice on confidential information, December 2014<br>NHS Care Records Guarantee<br>Anonymisation Standard for Publishing Health and Social Care Data<br><br>Crown Copyright: Data Protection Act 2018<br>UK General Data Protection Regulation<br>Department of Health: NHS Constitution<br>Information Governance Alliance: NHS Records management Code of Practice<br><br>Information Commissioner: |

| | |
|---|---|
| | Anonymisation Code of Practice<br>Subject Access Code of Practice<br>Employment Practices Code<br>Supplementary Guidance<br>Data Sharing Code of Practice |