CONTROLLED DOCUMENT

University Hospitals Birmingham
NHS Foundation Trust

Data Protection, Confidentiality and Disclosure Policy

CATEGORY:	Policy (Operational)
CLASSIFICATION:	Governance
PURPOSE:	This policy outlines the framework within which all Trust staff and stakeholders are required to work to ensure the Trust is compliant with data protection legislation and national best practice.
Controlled Document Number:	1171
Version Number:	2.1
Controlled Document Sponsor:	Deputy Chief Executive Officer Caldicott Guardian
Controlled Document Lead:	Information Governance Lead
Approved By:	Chief Executive
On:	25th January 2023
Review Date:	25th January 2026
Distribution: • **Essential Reading for:** • **Information for:**	All Staff who routinely access with sensitive or personal information All Staff

Contents

Version Control

Version	Title	Issue Date
1.0	Data Protection, Confidentiality and Disclosure Policy	08/07/2019
2.0	Data Protection, Confidentiality and Disclosure Policy	02/02/2023
2.1	Data Protection, Confidentiality and Disclosure Policy	06/02/2024

1 Policy Statement

The purpose of this policy and associated documents is to ensure that University Hospitals Birmingham NHS Foundation Trust (The Trust') complies with the Data Protection Legislation (as defined in Appendix B), as well as guidance issued by Department of Health and Social Care and the Information Commissioner in relation to confidentiality and information security.

2 Scope

2.1 This policy applies to all areas and activities of the Trust and to all individuals employed by the Trust including contractors, volunteers, students, locum/agency, bank staff and staff and individuals on honorary contracts.

2.2 This policy covers:

2.2.1 All aspects of information, including (but not limited to):

- Patient/Client/Service User information;
- Staff information; and
- Personal and special category data.

2.2.2 Structured and unstructured record systems - paper and electronic:

- Photographic images, digital, video recordings including CCTV;
- All information systems purchased, developed and managed by/or on behalf of, the organisation; and
- Trust information held on paper, mobile storage devices, computers, laptops, tablets, mobile phones and cameras.

2.2.3 All types of processing of information, including (but not limited to):

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

3 Definitions

Terms such as 'data controller', data processor' and 'processing' shall be given the meaning as defined in the Data Protection Legislation. A list of frequently referred to terms is contained in Appendix B of this policy.

4 Framework

4.1 This section describes the broad framework for the Data Protection, Confidentiality and Disclosure Policy. Detailed instructions are provided in the associated procedural documents.

4.2 The Deputy Chief Executive Officer (DepCEO) or Caldicott Guardian (or their deputies) shall approve procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

4.3 The Trust will meet its obligations to comply with Data Protection Legislation and other guidance/standards on confidentiality and information security through this policy to ensure that:

4.3.1 All members of staff are aware of, understand and fully comply with the Data Protection Legislation;

4.3.2 All members of staff with responsibility for processing patient-identifiable information, are aware of and comply with the Caldicott principles; and

4.3.3 There are procedures and processes in place which mitigate data protection/information security breaches and that any such breaches are properly investigated, and lessons learnt shared across the organisation as appropriate.

4.4 The Trust recognises the benefit and need to share personal information with other health/social care organisations and other agencies in a controlled manner which is consistent with the interests of those individuals whose personal information is being shared and/or the public as a whole.

4.5 Data Protection Legislation

4.5.1 The Data Protection Legislation established a framework of rights and duties which are designed to safeguard personal data. The framework balances the legitimate interests of organisations to collect and use personal data for business purposes against the right of individuals to respect for their privacy, as enshrined in Article 8 of the Human Rights Act 1998.

4.5.2 The UK Data Protection Legislation is composed of the following:

a) UK GDPR is the UK version of the EU GDPR and sets out the general principles of processing of personal data.

b) Data Protection Act (DPA) 2018 sets out the conditions under which special categories of personal data (including healthcare data), as well as any exemptions and derogations from UK GDPR.

4.5.3 Data protection is concerned with the fair and proper use of information about people. It is about treating people fairly and openly, recognising their right to have control over their own

identity and their interactions with others, and striking a balance with the wider interests of society.

4.5.4 Data protection is essential for supporting innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

4.5.5 It follows that any data processing activities such as collecting, using, storing, viewing, sharing/disclosing or disposing of personal data may only be conducted where there is a legal basis to do so and only to the extent necessary associated with that legal basis.

4.5.6 Legal bases include, but are not limited to, the public interest in the provision of healthcare, the Trust's duties as an employer and consent by the data subject. Not all legal bases allow the processing of especially sensitive (special category) data such as healthcare data. Staff must therefore seek advice from the Information Governance Department (IG) where they are wishing to set up a new process involving personal data (see below DPIA).

4.5.7 Legal basis:

a) For the provision of care, the Trust does not require the explicit consent of patients and can instead rely on Article 6(e) UK-GDPR ("processing is necessary for the performance of a task carried out in the public interest") and Article 9(h) GDPR ("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 […]".

b) For secondary use/non care provisions, where the use of their information is not in connection with direct care, then a specific legal basis for that use must exist. This may be explicit consent or some other legal basis for that use.

4.5.8 This does not however, authorise the Trust to use patient data in any way it sees fit and in some instances patient consent might be required, therefore patients must be informed about:

a) The use and disclosure of their information and records;

b) The choices they have and implications of choosing to limit how information may be used or shared;

c) The details of the necessary information shared when care is to be provided by partner agencies and organisations; and

d) The potential use of their information for improvement of the quality and type of care they have received.

4.5.9 Much of this is managed through the Trust Privacy Notice for patients, which outlines the purpose and way in which information might be shared, who the data will be shared with, how long the data will be retained, the rights of the data subject (including opt-outs) and what security measures are in place to protect the data.

4.5.10 Similarly, the Privacy Notice for staff outlines the purpose and way in which staff information might be shared, who the data will be shared with, how long the data will be retained, staff subject access rights of the data subject and what security measures are in place to protect the data.

4.5.11 Both Patient and Staff Privacy Notices are available on the Trust website.

4.6 Caldicott Principles

4.6.1 The Caldicott Principles are a set of principles specific to the use of patient data within the NHS and they set out 8 best practice principles:

1. Justify the purpose(s) for using confidential information;

2. Use confidential information only when it is necessary;

3. Use the minimum necessary confidential information;

4. Access to confidential information should be on a strict need-to-know basis;

5. Everyone with access to confidential information should be aware of their responsibilities;

6. Comply with the law;

7. The duty to share information for individual care is as important as the duty to protect patient confidentiality;

8. Inform patients and service users about how their confidential information is used;

4.6.2 A full list of the Caldicott Principles and underlying rationale can be found in Appendix C.

4.7 Duty of confidentiality

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

a) A legal obligation derived from case law of Common Law Duty of Confidentiality;

b) A requirement established within professional codes of conduct;

c) Patient's right to confidentiality continues after their death; and

d) Included within all NHS staff contracts of employment.

4.7.2 Patients entrust staff with information regarding their health and other matters as part of their treatment. They do so in confidence and have the legitimate expectation that staff will respect their privacy and act appropriately. It is essential that the trust of patients is retained and that the Trust is seen to provide a confidential service to its patients.

4.7.3 Breaches of confidentiality; including inappropriate accessing, disclosure or use of health or staff records, or abuse of computer systems may lead to regulatory investigations and sanctions, legal proceedings, bring the Trust into disrepute, and can ultimately result in disciplinary measures to those who have negligently caused the breach.

4.8 Data Protection Impact Assessment

4.8.1 A Data Protection Impact Assessment (DPIA) is a process which helps the Trust to identify and minimise the data protection / privacy risks of any new project / process or change to existing processes/systems.

4.8.2 Initially, a screening tool will be used to understand whether a full scale DPIA is required. A full scale DPIA is a comprehensive exercise which will:

a) Describe the nature, scope, context and purposes of the processing;

b) Assess necessity, proportionality and compliance measures;

c) Identify and assess risks to individuals; and

d) Identify any additional measures to mitigate those risks.

4.8.3 Finalised DPIAs must be approved by either the Digital Health Group (for patient data) or IG Group (for staff data). The SIRO and Caldicott Guardian have the authority to sign off DPIAs outside of these meetings. DPIAs which are considered low risk, may be signed off by the Information Governance Lead or Head of Operational Support.

4.8.4 Where the Trust is involved in the development, testing, validation and/or deployment of artificial intelligence (AI) / machine learning tools, the ICO AI and data protection risk toolkit must be completed.

4.8.5 Staff involved in the deployment of new technology are reminded that additional steps might be required to ensure such technology is clinically safe and meets relevant cyber security, interoperability and accessibility standards. It may therefore also be necessary to engage with IT/IT Security team and one of the Clinical Safety Officer.

4.8.6 The IG Department will maintain a library of documentation to support staff in the aforementioned processes (DPIA Procedure and its supporting documentation are available on Trust intranet site).

4.9 Third Party Due Diligence

4.9.1 Where the project/process utilises a third-party organisation (e.g., system supplier, or consultancy firm) the Trust is required to undertake a due diligence exercise on them prior to allowing them to process any personal data.

4.9.2 As part of the due diligence, the third-party organisation is assessed in terms of data security, integrity and confidentiality.

4.9.3 Any findings of the due diligence assessment will feed into the contract with that party to ensure that risks are sufficiently mitigated.

4.10 Protective Measures (Security)

4.10.1 As part of current Data Protection Legislation, the Trust is required to comply with technical and organisational measures (protective measures) which ensure the confidentiality, integrity and availability of data and resilience of systems and services.

4.10.2 There is currently no definitive list of such protective measures, as these change over time and depend on the type of service delivered and data to be protected. Organisational measures include policies, procedures, contracts, standard operating procedures and codes of conduct. Commonly known technical measures include encryption and pseudonymisation of datasets. Other technical measures take the form of accreditations such as ‘Cyber Essential’ or ISO 27001.

4.10.3 The Trust holds some of these certified accreditations for defined services (e.g., ISO 27001 for QEHB IT email services) and has a series of policies and procedures in place which staff are expected to adhere to which are referenced below.

4.10.4 The Trust will further ensure that any third party who processes personal data on behalf of the Trust either has appropriate accreditations or adequate internal controls given the nature of the data to be protected, the harm which might result from a

breach, the state of technological development and the cost of implementing such measures.

4.11 Access to information

4.11.1 Access to personal information is restricted. Staff should only have access to personal information or create records containing personal information where it is necessary in order to carry their roles in the Trust.

4.11.2 Staff are prohibited from accessing or using patient information for personal reasons, or where there is no justification/legitimate reason for doing so, e.g., accessing information of family members, friends, celebrities, colleagues/neighbours, where they are not involved in that person's direct care. Any member of staff who fails to maintain acceptable standards of conduct in accordance with accessing information and /or Trust disciplinary standards may be subject to disciplinary action.

4.11.3 The list below is not exhaustive, however, provide examples where access or using patient information can be justified / with legitimate reasons.

- For care - where the staff member has a legitimate relationship with a patient i.e., the staff member is involved in providing care to the patient, or is a member of the health care team treating the patient. This includes both health care professionals and administrators e.g., ward clerks, and receptionists.
    - Clinical auditors accessing patient information for use in registered audits;
    - Clinical coding staff for coding purposes;
    - Medical Records team accessing information as part of their duties, e.g., booking clinics;
    - Investigators where the Trust has commissioned an investigation for a reported incident;
    - Managers to organised and arrange care for patients e.g. discharge and transfer
- For HR issues - where the staff member is the line manager of a staff member, or is authorised to access personal files e.g., HR, etc. Where the staff member is authorised to access personal data/create records in specific circumstances where there is a justified reason for doing so, for example:
    - Legal services or complaints staff accessing information for medico-legal cases and complaints.

- Finance staff accessing information for financial transaction purposes;
- Research team accessing information where patients have consented for their data being used;
- Informatics staff processing information of patients who have not opted out for their data being used for planning and improvement of service provided;
- Data Quality team accessing information for reviewing, identifying and correcting data quality errors; and
- IT staff with responsibility for maintaining and monitoring IT systems.

4.11.4 Staff who are patients of the Trust must not access medical information about themselves, other than through raising a request through the Subject Access Team of Medical Records, in line with the Subject Access process, or through other authorised methods, e.g., a patient portal.

4.12 Secondary Use of Information

4.12.1 As already explained in section 4.11, any data processing activities can only be conducted where there is a legal basis or justification for doing so.

4.12.2 Where an activity goes beyond the initial legal basis, an additional legal basis must be available, or the activity is illegal. For instance, identifiable patient information can only be used for research activities if such research meets the additional requirements set by the Data Protection Legislation. This means that either patient consent or section 251 Confidentiality Advisory Group (CAG) approval must be obtained. Other examples include the use of information for teaching purposes or publications.

4.13 National Opt-Out

The National data opt-out is a service that allows patients to opt out of their confidential patient information being used for research, planning and other secondary use cases (that is purposes which go beyond the direct care of patients). All information asset managed and processed by the Trust must be compliant with the national data opt out. Please refer to the national data opt out guidance or obtained further advice from IG.

4.14 Sharing Information

4.14.1 The Trust is required to share information about patients and staff for various reasons. When necessary, Data Sharing/Processing Agreements will be completed prior to any information being

shared/transferred and signed by an authorised signatory in accordance with the Trust's Scheme of Delegation. The basis of such agreements will be the DPIA, which will have considered the risks and put in place the necessary mitigating protective measures (see section 4.10).

4.14.2 Where the sharing of information is for purposes other than direct healthcare, the Trust must have another legal basis to do so. This may be consent by the data subject but could also be a court order or overriding public interests. The IG Department will ensure that each legal basis has been considered in full and will discuss the request/need to share information with appropriate personnel such as Caldicott Guardian and/or SIRO.

4.15 Disclosure of Information Outside the United Kingdom (UK)

4.15.1 It is a legal requirement under Data Protection Legislation not to disclose or transfer any personal data outside the UK to a country or territory which does not ensure an adequate level of protection, unless certain exemptions apply, or adequate protective measures are taken.

4.15.2 Certain countries and territories have been awarded with UK adequacy regulations and are thus considered safe; a full list can be found on the ICO website. In the absence of an adequacy decision the Trust must carry out 'transfer impact assessment' and identify appropriate safeguards as defined in the UK GDPR before making restricted transfer. In the absence of both adequacy decision and appropriate safeguards the Trust will have to rely on one of the 8 exemptions as set out in Article 49 GDPR.

4.15.3 Due to the complexities of these data transfers, the Information Governance Department must be consulted prior to entering into any agreement to transfer or process personal data outside of the UK.

4.16 Destruction/disposal of data

4.16.1 Confidential data must be destroyed in a secure manner once it meets the criteria to be destroyed. All information held by the Trust must be destroyed in accordance with Trust approved process as detailed in the Trust's Record Management Policy and associated procedures.

4.16.2 Any information held in a paper or plastic format must be destroyed via the Trust's approved process of disposal for confidential and office paper waste, and/or plastic patient ID.

4.16.3 Where information is held on electronic media/hardware and the removable media needs to be destroyed or replaced this must follow the Digital Equipment Disposal Procedure.

5 Duties

5.1 Caldicott Guardian

The Trust's Caldicott Guardian has particular responsibility for reflecting patients' interests regarding the use of patient identifiable data. They are responsible for ensuring that patient identifiable data is used and shared in an appropriate and secure manner. The Trust's Chief Medical Officer shall appoint staff to act as a Caldicott Guardian/ Deputy Caldicott Guardian.

5.2 Senior Information Risk Owner (SIRO)

5.2.1 The Chief Strategy and Digital Officer is the Senior Information Risk Owner, who is also the named Executive responsible for Data Protection. The SIRO will provide assurance to the Board of Directors on compliance with this policy. The Director of Legal Services and Regulatory Compliance is the Deputy Senior Information Risk Owner.

5.2.2 The SIRO is the owner of the Trust's Information Asset Framework and Register. For more information, please refer to the Information Asset Procedure.

5.3 Data Protection Officer (DPO)

The DPO is responsible for overseeing the Trust's strategy for data protection and implementation to ensure compliance with Data Protection Legislation requirements. The DPO directly reports to the Trust SIRO. The DPO will assist the Trust to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding high risk Data Protection Impact Assessments (DPIAs) and act as a senior contact point for data subjects.

5.4 Information Governance Group (IGG) - Chaired by SIRO

5.4.1 The Chair of the Information Governance Group is responsible for ensuring this policy is effectively implemented along with supporting guidance and national best practice. The Chair is also responsible for ensuring there is a robust training programme in place to support staff in their responsibilities and for monitoring the implementation of this policy.

5.4.2 The Chair of IGG is responsible for ensuring the review and ratification of the Trusts annual submission of the Data Security and Protection Toolkit.

5.4.3 IGG reports to the Board of Directors via the SIRO.

5.5 Site Representatives

Each site is required to nominate a formal lead to act as a representative for IG matters in the site. They will attend an appropriate IG assurance meeting, provide regular reports and updates, and ensure dissemination of information within their site. They will also monitor training and incident management and provide assurance that work is being carried out in line with policy and procedure.

5.6 Information Asset Owners (IAOs)

Information Asset Owners (IAOs) are accountable to the SIRO and must provide assurance that information risks are being managed effectively in respect of the information assets/systems that they own. IAOs may choose to appoint Information Asset Administrators (IAAs) who will have day to day responsibilities for control of information assets reportable to the IAOs.

5.7 Information Governance Lead

The Information Governance Lead is responsible for ensuring that the DPA, Caldicott principles and duty of confidentiality are fully observed within the Trust. They are responsible for:

5.7.1 Ensuring that training is available to staff in accordance with the Mandatory and Statutory Training Policy;

5.7.2 Ensuring compliance with requirements from the Information Commissioners Office, including notification of incidents.

5.7.3 Advising on and updating policies in relation to guidance from the ICO, Department of Health or other relevant organisations;

5.7.4 Raising awareness of data protection and confidentiality issues to staff of all levels;

5.7.5 Providing expert guidance to staff regarding legislation, relevant policies, procedures and good practice; and

5.7.6 Ensuring data protection and confidentiality breaches are investigated in conjunction with the Operational Site or relevant Corporate department.

5.8 All Managers

All Managers are responsible for ensuring that:

5.8.1 Staff are aware of this policy;

5.8.2 This policy is incorporated into local processes;

5.8.3 Staff remain compliant with IG training requirements; and

5.8.4 Any breaches, or suspected breaches, of data protection or confidentiality are reported in line with the Trust's Incident Reporting procedure.

5.9 All Staff

All staff must:

5.9.1 Comply with this policy and associated procedures;

5.9.2 Adhere to the standards set out in the NHS Code of Practice on Confidentiality, which is a guide to the required practice for those who work within or under contract to the NHS;

5.9.3 Ensure compliance with the terms of their contract of employment, which includes clauses in relation to confidentiality and data protection;

- Health professionals working in the NHS are bound by professional codes of conduct in respect of confidentiality.

5.9.4 Ensure any breach, or suspected breach, of this policy is reported via the online incident reporting system and in accordance with the Trust's Incident reporting procedures.

5.9.5 All staff also must:

a) Understand the Trust's obligations under current Data Protection Legislation;

b) Be able to signpost patients to where they can find further information about the Trust's data processing activities;

c) Ensure information kept is current and up to date;

d) Ensure they are compliant with appropriate training to support them with the implementation of this policy; and

5.9.6 <u>not</u>:

a) Share more information than is necessary for fulfilling the purpose;

b) Use identifiable information if the purpose can be satisfied by using anonymised or pseudonymised information;

c) Access records of friends, relatives, neighbours or colleagues unless they have a legitimate relationship;

d) Access their own medical records;

e) Ignore breaches of this policy; or,

f) Disclose information to the public domain, e.g., social media platforms.

6 Implementation and Monitoring

Implementation

6.1 This policy will be available on the Trust's intranet site. The policy will also be disseminated through the management structure within the Trust and advertised to all staff.

6.2 All staff are mandated to undertake training in data protection and confidentiality on an annual basis through Information Governance mandatory training sessions (face to face and e-learning)

Monitoring

6.3 Monitoring of compliance of this policy will be undertaken using the Data Security and Protection Toolkit. This is a self-assessment completed annually and signed off by the Information Governance Group and the Board of Directors. Evidence on standards compliance will be reported annually to the Audit Committee.

6.4 Appendix A provides details on how this policy will be monitored.

7 References

7.1 Legislation

Data Protection Act 2018

EU General Data Protection Regulation 2016
UK General Data Protection Regulation (UK GDPR) 2018

Access to Health Records 1990
Access to Medical Reports Act 1988

Computer Misuse Act 1990

Criminal Justice and Immigration Act 2008

Freedom of Information Act 2000

Health and Social Care (National Data Guardian) Act 2018

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

7.2 NHS related Guidance

Caldicott Review 2016 (National Data Guardian Security Standards)

Confidentiality: NHS Code of Practice

Digital Technology Assessment Criteria (DTAC)

Guide to the General Data Protection Regulation

ICO AI and data protection risk toolkit

ICO The Employment Practices Code

Information Security Management: NHS Code of Practice

National data opt-out - NHS Digital

Records Management: Code of Practice for health and social care 2022

8 Associated Policy and Procedural Documentation

Access to Health Records Procedure

Digital Equipment Disposal Procedure.

Freedom of Information Act and Environmental Information Regulations Policy

Information Asset Procedure

Informatics Data Quality Policy

Information Security and Access Control Policy

Mandatory and Statutory Training Policy

Photographic and Video Recording Consent and Confidentiality Policy and Procedure

Records Management (Corporate and Clinical) Policy and associated procedures

Trust Sponsored Research Policy

Appendix A **Monitoring Matrix**

Monitoring	Lead	Reported To	Process	Frequency (Minimum)
Data Security and Protection Toolkit	IG Lead	IGG	Self-assessment completed annually. Evidence will be collected to support the standards and an annual report regarding the process for sign off will be made.	Quarterly and annually
Incident Reporting and Management	IG Lead	IGG	Report to IGG on incident numbers, themes and actions.	Quarterly
Staff Training	IG Lead	IGG Site Leads	All staff are mandated to undertake training in data protection and confidentiality annually through information governance mandatory training sessions (face to face and e-learning). Site Leads receive monthly report from Learning and Development	Quarterly
Compliance Audits	IG Lead	IGG	Rolling series of compliance audits (consist of self-assessment audit and IG visits) throughout the Trust. Reports are sent to all Leads and any high risks are escalated as appropriate. Report to IGG	Biannual
Board reporting	Director of Legal Services and	Trust Board	Annual report to Trust Board covering Data Protection compliance in the Trust including DSPT status.	Annual

	Regulatory Compliance			

Appendix B DEFINITIONS

Controller shall take the meaning given in the Data Protection Legislation;

Data Guidance means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation to the extent published and publicly available or their existence or contents have been notified to the Data Processor by NHS England and/or any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by NHS Digital, the National Data Guardian for Health & Care, the Department of Health, NHS England, the Health Research Authority, Public Health England, the European Data Protection Board and the Information Commissioner;

Data Protection Impact Assessment means an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Protection Legislation means (i) the UK GDPR (ii) the DPA 2018 (iii) all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR);

Data Protection Officer shall take the meaning given in the Data Protection Legislation;

Data Subject shall take the meaning given in the Data Protection Legislation;

Data Subject Access Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

GDPR means either the UK GDPR or General Data Protection Regulation (Regulation (EU) 2016/679);

Information Commissioner means the ICO which is the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals , and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection Legislation;

Personal Data shall take the meaning given in the Data Protection Legislation;

Personal Data Breach shall take the meaning given in the Data Protection Legislation;

Processor shall take the meaning given in the Data Protection Legislation;

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures.

Pseudonymisation: Pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

Appendix C THE CALDICOTT PRINCIPLES

1. **Justify the purpose(s) for using confidential information**

   Every proposed use or transfer of confidential information should be clearly defined and scrutinised, with continuing uses regularly reviewed, by the IG.

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.

3. **Use the minimum necessary confidential information**

   Where use of the confidential information is considered to be necessary, each item of information must be justified so that the minimum amount of confidential information is included as necessary for a given function.

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.

5. **Everyone with access to confidential information should be aware of their responsibilities**

   All staff; both clinical and non-clinical, handling confidential information should be fully aware of their responsibilities and obligations to respect patient confidentiality.

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.

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 their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

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.