Data Protection Policy

Contents

1. Version Control 3
2. Equality Statement 4
3. Vision and Values 4
4. Policy on a Page: Data Protection Policy 5
5. Introduction 6
6. Purpose 6
7. Scope 6
8. Policy Content 7
9. Guidance to Staff 9
10. Roles and responsibilities 13
11. Dissemination 14
12. Compliance and Monitoring 14
13. Review 14
14. Related Documents 14

Appendices 15

15. Appendix 1: Definitions of key terms used 15
16. Appendix 2: Equality Impact Assessment Form 16

Data Protection Policy

1. Version Control

Policy Title	Data Protection Policy
Version number	2.
Reference	CORP035
Category	Corporate
Target Audience	All North London NHS Foundation Trust Staff
Approved by (Step 1)	Chief Digital and Information Officer (CDIO).
Ratified by (Step 2)	Joint Information Governance Steering Group
Executive Director	Sarah Wilkins, CDIO and SIRO (Senior Information Risk Officer)
Date Ratified	30 September 2024
Date of Next Review	3-year cycle
Policy Author	Martin Nakasala
Email contact	Martin.Nakasala@nhs.net
Reviewed by	Pera Svilar
Key words	Data, Confidentiality, Integrity, Availability

Key changes to policy document

Version	Date	Summary of key changes
V 2.0	30/09/2024	Single Partnership policy put in place to replace BEH and C&I Data Protection Policies
C&I V.8	2024	C&I Data Protection Policy
BEH V.6	2024	BEH Data Protection Policy

2. Equality Statement

All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on equality and fairness.

All policy documents will be equality impact assessed and this will include equality and human rights with regard to the protected characteristics including age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex (gender) and sexual orientation.

The Trust will make accessible versions of this document available where requested by members of the public, service users or staff.

3. Vision and Values

We are guided in all we do by our **vision** and **values** and all policies and procedures are written in line with them.

Our **vision** is better mental health, better lives, better communities.

Our **values**:



4. Policy on a Page: Data Protection Policy

What does the policy cover?

- Data Protection
- Data Protection Legislation
- Data Processing
- Staff responsibilities in data protection.
- Confidentiality

Summary of what has changed since the last version.

- Moved policy to NLFT template.
- Merged the C&I and BEH Data Protection Policies.

To whom does the policy apply?

- All Trust Staff
- Patients and Service Users
- Contractors
- Third-Party Providers
- Suppliers

Who can I contact?

- Chief Digital Information Officer / Senior Information Risk Owner.
- Head of Information Governance / Data Protection Officer
- Information Governance

What training is available?

- The Trust will maintain a training needs analysis and provide appropriate training for staff with specialist roles.
- Data Security Protection training is mandatory for all staff.
- E-learning is available on the Electronic Staff Record (ESR) training platform or an alternative approved method of learning.

5. Introduction

As a prerequisite for complying with legislation and NHS England Digital standards, this document sets out the Trust's policy to be followed in relation to data protection. The Trust holds and processes information about its employees, patients, and other individuals for various purposes.

Information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The General Data Protection Regulations (GDPR) and the Data protection Act are the two pieces of law which underpin and govern how we manage, store and process personal data. They apply to both manual and electronically held data. We are the guardians of personal and sensitive information, and we must ensure it is kept safe and managed correctly to ensure trust and confidence in our organisation, and the wider NHS, is maintained.

6. Purpose

The primary purpose of a data protection policy is to provide a clear framework for the safeguarding of personal information within an organization. It aims to comply with legal requirements, such as the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, and to foster trust between the organization and its service users, employees, and partners by demonstrating a commitment to data privacy.

7. Scope

'Staff' in the Trust refers to:

• All salaried employees - full-time and part-time, including those on fixed term contracts.

• Associated persons - such as volunteers, secondees, those with honorary and zero-hours contracts.

• All prospective employees - including those who are part-way through recruitment who are undergoing pre-employment checks and those awaiting a start date.

• Contractors and sub-contractors including consultants.

• Agency and locum staff.

• Committee, sub-committee and advisory group members, and members of other such forums, who may be formally or informally appointed and not be directly employed or engaged by the Trust.

This Policy entails all personal data, and special categories of personal data held by, or on behalf of, the Trust, its processing, storage, handling, and usage. Such data includes but is not limited to:

• employee and staff records.

• patient data and records.

• personal data relating to volunteers working with the Trust.

• personal data in all formats including, but not limited to, paper copy, digital records, and CCTV.

8. Policy Content

8.1. Data protection Overview

The Trust's compliance with the Data Protection Act 2018 (DPA), and the UK General Data Protection Regulations (GDPR) ensures that it treats personal data in a confidential manner. A principle aim of the GDPR is to promote openness in the processing of personal data and therefore the Trust must ensure that Data Subjects know the reason their information is collected, its uses within the organisation and to whom, and the circumstances when, it may be disclosed.

The DPA and the GDPR can only be applied to records relating to living individuals. However, a duty of confidence is still owed to the deceased and their families. Please read Access to Health Records Act 1990 and the Common Law Duty of Confidentiality to provide guidance on this type of data.

Principles of the Data Protection Act:

• Lawfulness, fairness, and transparency - processing must be lawful, fair, and transparent.
• Purpose limitation - purposes of processing must be specified, explicit and legitimate.
• Data minimization - personal data must be adequate, relevant, and not excessive.
• Accuracy - personal data must be accurate and kept up to date.
• Storage limitation - personal data must be kept for no longer than is necessary.
• Integrity and confidentiality (security) - personal data must be processed in a secure manner.
• Accountability - take responsibility for what you do with personal data and how you comply with the other principles.

The DPA 2018 makes provisions for those conditions set out in the UK GDPR for the processing of any personal data. It also makes a distinction between personal data and special categories (sensitive) data.

Caldicott Principles
The Caldicott Report of 1997 established a number of general principles that health and social care organisations should use when reviewing its use of client information and include:

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

Articles 6 and 9 of the GDPR provide further conditions for processing data.

8.2 Individuals' Rights

The GDPR gives rights to individuals in respect to their own personal data held by others. These are:

- The right to be informed - emphasises the need for transparency over how the Trust uses personal data.
- The right of access - Individuals have the right to access their personal data and supplementary information, timescales apply.
- The right to rectification - Personal data can be rectified if it is inaccurate or incomplete.
- The right to erasure - enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
- The right to restrict processing – under certain circumstances individuals have a right to 'block' or suppress processing of personal data.
- The right to data portability - allows individuals to obtain and reuse their personal data for their own purposes across different services, (conditions apply).
- The right to object – includes the right to object to processing for purposes of scientific/historical research and statistics.
- Rights in relation to automated decision making and profiling.

These rights are not absolute and will be each be dealt with on a case-by-case basis. Approval where necessary will be sought from the Caldicott Guardian and or the Data Protection Officer.

8.3 Privacy by Design and Default

The Trust ensures that all systems, services, products, and processes protect personal data. To assess the compliance of all new data processing activities, a Data Protection Impact Assessment (DPIA) must be completed. A DPIA is a process to help organisations identify and minimise the data protection risks of a project.

Employees shall complete a DPIA when seeking to process information that is likely to result in an elevated risk to individuals. Employees should ask the Data Protection Officer (DPO) for their advice on the DPIA and document it as part of the process. Once completed, the DPIA should be entered in the information asset register and should be circulated to all stakeholders.

8.4 Privacy Notice and Fair Processing

The GDPR requires that data controllers provide certain information to people whose data they hold and use. This is known as a Privacy Notice (PN).

The Trust shall provide PNs to all patients and all employees, identifying who the data controller is, including contact details for the DPO. The PN should also explain the purposes for which personal data is collected and used, how the data is used and disclosed, how long it is kept, and the controller's legal basis for processing.

A Statement of Fair Processing / Privacy Notice should also be provided on the Trust's website. This reflects the requirement for a Statement of Fair Processing set out in the recommendations of the Caldicott Review.

8.5 Network and Information Systems Regulation (NISR)

The Networks and Information Systems Regulation aims to raise the levels of overall security and resilience of network and information systems for Operators of Essential Services across the UK and defines a set of principles used to guide decision-making. These principles fall under four main objectives:

- **Managing Security Risks**: Ensure that appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.

- **Protecting Against Cyber Attacks**: Ensure that proportionate security measures are in place to protect essential services and systems from Cyber-attack.

• **Detecting Cyber Security Events**: Security defences should remain effective and detect Cyber Security events affecting, or with the potential to affect, essential services.

• **Response and Recovery Planning**: Have capabilities to minimise the impact of Cyber Security incidents on the delivery of essential services including the restoration of those services where necessary.

8.6 NHS Code of Practice

Under the NHS Code of Practice, individuals have a right to confidentiality. Further guidance regarding confidentiality can be found in the NHS Code of Conduct. Please refer to the 'NHS Code of Practice for Confidential Information' for further detail.

8.7 Lawfulness for Processing Personal Data

In accordance with the Data Protection Legislation, a data controller must have a valid lawful basis in order to process personal data. The conditions for lawful processing can be accessed here. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

8.8 Responsibilities of Individual Data Users

All employees of the Trust who record/process personal data must ensure that they comply with the requirements of the DPA and the GDPR. Any personal data should be kept securely. Personal data must not be disclosed verbally or in writing or otherwise to any unauthorised third party.

A breach of the GDPR or the Trust's Data Protection Policy may result in disciplinary proceedings. Contact the Information Governance team via the email beh-tr.information.governance@nhs.net for data protection advice when unsure.

9. Guidance to Staff

9.1 Authorised employees

Staff should only have access to personal data in the following circumstances:

• Where they participate in that person's healthcare.
• For personnel/HR issues, where the employee is authorised to access personnel files.
• Where the employee is authorised to access personal data in specific circumstances.
• Employees must never access their own medical record – copies of records need to be applied for from the Medical Records team whose email address is nlft.Information.Request@nhs.net.
• Employees must not access records of people they know (whether a relative or not) without a legitimate (see above) reason for doing so.

9.2 Access to Personal Data

There are procedures in place to ensure that appropriate access to care records systems is provided to those members of staff who require access as part of their role. If staff change role, they must ensure they inform IT to remove any legacy access that is no longer required in their new role.

All clinical records should be kept secure. All departments holding confidential files should have a locked filing cabinet for these records and access to the filing cabinet should be limited to authorised personnel.

Staff must never access their own medical record or information treated in confidence – copies of records need to be applied for from the Medical Records team or HR for Personnel files. Staff must also not access records of people they know without a legitimate reason for doing so.

9.3 Telephone

Text Messages

Key considerations when using text messages to communicate to service users are:

• If they consent for appointment reminder services, service users should be informed of what information will be included in standard SMS messages sent to them via the service.
• Text messages should not be used to convey sensitive information.
• Staff must confirm that the mobile phone number correct.
• Staff must confirm that the mobile phone receiving the text message is being used by the intended recipient of the message.
• WhatsApp should never be used to send confidential patient information.

Guidance when making a call to a service user:
Staff calling a service user should follow best practice and must not disclose who they are or where they are calling from to avoid inadvertently disclosing confidential information. If calling a service user, the script to follow is:

- Please can I speak to?
- Am I speaking to?

If it is not the service user then ask when they will be available and call back later, there is no need to leave any other details. If it is the service user first get them to confirm their name, address and DOB and cross check that this is correct with the records held before disclosing any information.

Please refer to the **Communications Policy** for further guidance.

9.4 Email

This section should be read in conjunction with the **Email policy**.

The Trust uses NHS Mail, a secure email system. Where email is used to send sensitive information, this should be clearly indicated in the subject header, for example marked ‘Confidential.’ If communicating with a patient via email, always gain consent and check the email address as part of the standard demographic checks when a patient attends the trust.

It is the responsibility of the Trust staff member to seek assurance from the recipient that their email is secure to receive confidential personal data. You can follow this link to access the list of accredited organisations.

9.5 Social Media

You must consider the potential impact on confidentiality, your own reputation, that of the Trust and the NHS in general. You are expected to behave responsibly, professionally and in accordance with your professional codes of conduct and the Trust's values and policies. Please refer to the **Communication Policy** for further guidance.

9.6 Post

Ensure that if correspondence contains any person-identifiable information, it is marked 'Private & Confidential' and is in a sealed envelope. Staff should ensure that post is sent to a named person. Patient identifiable information that is extensive (e.g., a set of copy records) or relates to more than one person should be sent by Recorded Delivery. Special Delivery should be used for extremely sensitive information or batches of information.

9.7 Photography/Filming

Please refer to the **Communications Policy** for detailed guidance on photography and video recording.

9.8 Confidential Waste

Confidential paper waste should be shredded. Ensure that all confidential waste is disposed of in the confidential waste bins / cross shredded.

9.9 Printers & Photocopying

- Use a confidential waste bin for spoiled prints and copying.
- Check that you have collected all your printing/copying and originals from the machine.

9.10 Sharing Information

Information shall be shared in accordance with the **Information Sharing Policy**.

Information Sharing Agreements are agreed at organisational level and are signed by the Caldicott Guardian, while non-Disclosure Agreements are agreed at personal level (e.g., contract staff) and are signed off by the Head of Information Governance.

9.11 Security and Confidentiality Breaches

Security and Confidentiality Breaches of data protection law are managed as per the IG Incident Management Policy. Confirmed breaches must be reported to the Information Commissioner's Office within 72 hours of becoming aware of the incident. The Information Governance Team will provide investigating officers with advice on suspected breaches of confidentiality.

9.12 Patients' Right of Access to Medical Records

An individual who wishes to exercise his/her right of access to their medical records are asked to formally request this information in writing to the Medico Legal Health Records Team who will provide an application form. Please refer to the Subject Access Request policy.

9.13 Staff Right of Access to Personal Records

Employees wishing to access their personal data should put their request in writing to the Information Governance Team. Please refer to the Subject Access Request policy.

9.14 Disclosure outside the UK and EEA (European Economic Area)

Personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed, or transferred outside the EEA. For clarification, please contact the Information Governance Manager.

9.15 Retention of Data

Records will be stored securely for the appropriate length of time in accordance with the Department of Health's Records Management Code of Practice 2021.

9.16 Chaplaincy

Data concerning a person's health, and data concerning religious or philosophical beliefs, are a class of "special category data." The processing of special category data is prohibited unless a ground for processing that data can be identified. The processing and sharing of data about patients for the purposes of providing chaplaincy services will involve data concerning a patient's health or religion.

9.17 NHS National Data Opt-Out

This national policy enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in the Review of Data Security, Consent and Opt-Outs. Please refer to the **National Data Opt-out Policy** for further guidance.

9.18 Paper Diaries

Paper diaries in which patient data is recorded must not be used by patient contact staff. Instead, staff must use the electronic diaries in RiO. For further guidance, please refer to the **Records Management and Information Lifecycle Policy.**

9.19 General Security

• Do not allow unauthorised people into areas where confidential information is held unless they are supervised.

• Do not share door security codes with unauthorised people.

• Operate a clear desk policy. Do not leave confidential information out overnight.

• Wear your Trust identity badge so that other members of staff know who you are.

• Gain patient consent before sharing personal information with relatives or friends.

• Any medical notes should be checked by clinicians before patients see them, to check for any information that might cause the patient harm or distress to read.

• Forward any requests from patients for copies of their notes to the Medical Records team.

• Personal data or any other confidential data stored in a paper format is not to be taken off-site unless you are authorised to do so.

• When taking Trust equipment and belongings off site, store them in the boot of the car whilst travelling or in transit. You must not under any circumstances leave personal or confidential patient information in your vehicle overnight.

9.20 Cyber Security

Please refer to the Information Security Policy for holistic guidance on cyber security. If staff receive suspicious email from unknown sources, they should:

• Not click on links or open attachments.
• Send the email, **as an attachment**, to the following email: spamreports@nhs.net
• Delete suspicious emails – do not reply.

9.21 NHS Counter Fraud Authority

This is concerned with dealing with requests for information from the NHS Counter Fraud Authority or Local Counter Fraud Specialist (LCFS) in the prevention, detection, and investigation of potential or actual crime. The Trust must co-operate with the CFSMS under these circumstances and can do so without the data subject's consent.

9.22 Police

All requests from the police for personal data will be dealt with on a case-by-case basis via the IG Manager, Head of Information Governance or Caldicott Guardian, who will decide if the information can be disclosed.

10. Roles and responsibilities

	Role	Responsibility
1.	The Chief Executive	Overall responsibility for ensuring that mechanisms are in place for the overall implementation, monitoring and revision of policy
2.	Senior Information Risk Owner (SIRO)	The SIRO is the Chief Digital Information Officer. The SIRO ensures that identified information security incidents/risks are followed up and incidents managed. They ensure that the Board is briefed on all GDPR issues. The Trust's Deputy SIRO and Data Protection Officer support the role.
3.	Caldicott Guardian (CG)	Support implementation of processes and procedures to ensure confidentiality and data protection are properly embedded within the organisation.
4.	Data Protection Officer (DPO)	DPO for the Trust and responsible for confidentiality and security issues for all patients and staff.
5.	Information Asset Owners (IAO)	IAOs for each Division will nominate an individual who consults with the IG Team regarding their data flow activities on a regular basis.

	Role	Responsibility
6.	All Staff	•Undertake annual mandatory Information Governance training and understand and comply with their duties and responsibilities. •Report Data Protection and Confidentiality related incidents including data breaches through the trust incident reporting tools Datix / Ulysses and •Escalate any data protection and confidentiality related concerns through their Line management and / or to the IG Lead

11. Dissemination

All approved policies will be uploaded onto the staff intranet and updated on the policy register.

12. Compliance and Monitoring

Lead	Method for monitoring compliance	Frequency	Committee or Group responsible for implementation	Committee or Board to receive assurance
Head of Information Governance	Completion of DSPT	Annual	Information Governance	Joint IGSG
	Trust Complaints and Incidents Audit	Six monthly	Information Governance	Joint IGSG
Information Asset Owner	Completion of DPIAs	For new data processing	Information Governance	Joint IGSG
IG Manager	Review entries on Datix	Monthly	Information Governance	Joint IGSG
	Data Protection and Confidentiality Audits.	Quarterly	Information Governance	Joint IGSG

13. Review

The policy shall be reviewed at least every three years from the date of approval.

14. Related Documents

• Information Sharing Policy
• Information Security Policy
• Communications Policy
• Information Risk Policy
• Records Management and Information Life Cycle Policy
• Information Governance Incident Management Policy
• Consent to Treatment Policy
• National Data Opt-out Policy
• Email Policy
• Subject Access Request Policy
• Data Protection Impact Assessment (DPIA) Policy
• A guide to lawful basis | ICO
• The secure email standard - NHS England Digital
• Code of practice on confidential information - NHS England Digital

Appendices

15. Appendix 1: Definitions of key terms used

Personal data means any information relating to an identified or identifiable natural person ('data subject').

Data Breach is where there is breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Special categories (Sensitive) of personal data – types of information that are considered sensitive and require extra protection under data protection legislation.

Information Assets means any electronic or paper records such as service evaluation, customer/patient complaints, clinical and research records.

Processing - includes obtaining, recording, holding, obtaining, sharing, using the information or data, or conducting any operation or set of operations on the information or data.

Data Subject – "a living individual who is the subject of the personal data."

Data Controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed.

Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Third party – Natural or legal person, public authority, agency, or body other than the data subject, controller and processor who is authorised to process personal data by the controller or processor.

Consent – A**ny freely given, specific, informed, and unambiguous indication of the data subject's wishes** by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Impact Assessments (DPIA) – A DPIA is a process designed to help you systematically analyse, identify, and minimise the **data protection risks of a project or plan.**

The Caldicott Principles – A set of guidelines that help health organisations ensure proper treatment of patient-identifying information.

16. Appendix 2: Equality Impact Assessment Form

1. Expected impact of proposal on people with protected characteristics Just because a policy or initiative applies to all, does not mean it will have an equal impact on all			
Characteristics	**Positive**	**Neutral**	**Negative**
Age	☐	☑	☐
Disability	☐	☑	☐
Race	☑	☐	☐
Gender re-assignment	☑	☐	☐
Religion/Belief	☑	☐	☐
Sex (male or female)	☐	☑	☐
Sexual Orientation	☑	☐	☐
Marriage and civil partnership	☑	☐	☐
Pregnancy and maternity	☐	☑	☐
The Trust is also concerned about addressing health inequalities for other disadvantaged groups			
Carers	☐	☑	☐
Part-time staff	☐	☑	☐
Socio-economic	☐	☑	☐
Homeless people (SUs)	☐	☑	☐
Unemployed people (SUs)	☐	☑	☐
Substance misuse (SUs)	☐	☑	☐

2. Consideration of available data, research and information

- Use this section to demonstrate an understanding of who could be affected by the proposal. Include general population data where appropriate, and information about people who will be affected with reference to protected and other relevant characteristics.
- For each evidence source and say which characteristic(s) it relates to. You can include a mix of qualitative and quantitative data e.g., from national or local research, available data. Include the main findings of any engagement and consultation
- Outline whether there is any over or under representation of equality groups within relevant services - don't forget to benchmark to the local population where appropriate.
- For workforce / management of change proposals you will need to look at the diversity of the affected teams using available evidence such as HR reports which shows the diversity profile of council teams and service areas. Identify any over or under-representation compared with NLMHP's' population economically active citizens for different characteristics. Additional sources of useful workforce evidence include: the Employee Staff Survey Report, WRES, WDES, Gender Pay Gap Reports etc.
- Where there are gaps in the evidence, or you don't have enough information about some equality groups, include an equality action to find out in question 4. This doesn't mean that you can't complete the assessment without the information, but you need to follow up the action and if necessary, review the assessment later.
- If you are unable to fill in the gaps, please state this clearly with a justification.
- For workforce related proposals all relevant characteristics may not be included in HR diversity reporting (e.g., pregnancy/maternity). For smaller team's diversity data may be redacted.
- A high proportion of not known/not disclosed may require action to address under-reporting.

	Key questions	Your Response

	(Supports EDS Domains)	(Please reference data, research and information that you have reviewed which you have used to form your response)
2.1	What evidence, data or information have you considered to determine how this policy/development contributes to **delivering better health outcomes for all and improving patient access and experience??**	The Trust collects a lot of data / information, including health data which constitutes special categories of data that require greater protection. The trust also collects a lot of information about its staff, systems, and suppliers among several others. All these work together to enable us to deliver better health outcomes to the community. We therefore have to have policies in place that ensure proper handling and protection of the data / information.
2.2	What evidence, data or information have you considered to determine how this development/policy contributes to **delivering a representative and well supported workforce?**	Personal data, especially special categories of data, need to be protected from confidentiality, integrity and availability risks. Breach of such data can have a devastating impact on the data subjects. This policy aims to protect such data so all subjects can be protected from negative impacts.
2.3	What evidence, data or information have you considered to determine how this policy/guide/development contributes **to inclusive leadership and governance?**	This policy spells out responsibilities for all levels of Trust staff to ensure that data / information is protected at all times.

3. What involvement and consultation has been done in relation to this 'policy'? (e.g., with relevant groups and stakeholders)	
Response	Detail of involvement and consultation
Joint IG Steering Group	**19 September 2024** – Policy brought to IGSG meeting, and the Group requested for removal of duplication with other policies and to amend section on social media.
Head of Information Governance /Data Protection Officer	The Head of Information Governance / DPO requested for the policy to include information on paper diaries, how to contact patients by phone and on consent.
Information Governance Group	The IG group has been involved in agreeing what should be included in all the IG-related policies.

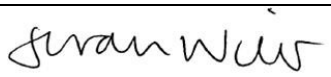
4. Equality Impact Assessment Improvement Plan

If your analysis indicates some negative impacts, please list actions that you plan to take as a result of this analysis to reduce those impacts or rebalance opportunities.

- These actions should be based upon the analysis of data and engagement, any gaps in the data you have identified, and any steps you will be taking to address any negative impacts or remove barriers.
- The actions need to be built into your service planning framework.
- Actions/targets should be measurable, achievable, realistic and time framed.

Group	Potential positive, neutral and/or negative impacts identified	Actions to mitigate any negative impact or enhanced policy	By whom
Age			
Disability			
Race			
Gender re-assignment			
Religion/ Belief			
Sex (male or female)			
Sexual Orientation			
Marriage and civil partnership			
Pregnancy and maternity			
Carers			

Group	Potential positive, neutral and/or negative impacts identified	Actions to mitigate any negative impact or enhanced policy	By whom
Serving or ex serving members of the Armed Forces			
Socio-economic (deprivation)			
Vulnerable groups (homeless, unemployed, substance misuse			

5. Sign off and publishing	
1. If this Equality Impact Analysis (EIA) relates to a policy, guide, procedure or protocol, please attach it to the policy/guide and process it through the normal approval process. 2. EIA's need to be accessible as they may be requested to support Freedom of Information (FOI), for publication on the Trust website, by the Equality, Diversity and Inclusion (EDI) Team requests or by the public or any other organisations etc. So, please ensure that your EIA's are stored in your department's shared folder. 3. Once you have completed this form, you need to sign it and state the name of the accountable manager, Head of Service or Director where appropriate. 4. The email for support to complete your EIA or for queries is: beh-tr.equalityimpactassessments@nhs.net	
Name/s, job title/s and contact/s details of person/s completing this assessment	
Name: Martin Nakasala	Position and Division: Information Governance Compliance Officer
Signed: mmnakasala	Date:
Name, job title and contact details of accountable person	
Name: Sarah Wilkins	Position: Chief Digital and Information Officer
Signed: 	Date: 18th October 2024