Data Sharing Agreement between London Borough of Camden and North London NHS Foundation Trust in respect of Camden Mental Health Individual Placement and Support Employment Services.

Contents

1. Introduction to the Sharing

This Data Sharing Agreement [DSA] documents how the parties to this agreement, listed in Appendix A, will share personal data about clients or beneficiaries of the Camden Mental Health Individual Placement and Support Employment Services. By signing this Agreement, the named agencies agree to accept the conditions set out in this document, according to their statutory and professional responsibilities, and agree to adhere to the procedures described.

This Agreement has been developed to:

- Define the specific purposes for which the signatory agencies have agreed to share information.
- Outline the Personal, Special Category and Criminal Data to be shared.
- Set out the lawful basis conditions under UK GDPR and Data Protection Act 2018 through which the information is shared, including reference to the Human Rights Act 1998
- Stipulate the roles and procedures that will support the processing/sharing of information between agencies.
- Describe how the rights of the data subject(s) will be protected as stipulated under the data protection legislation.
- Describe the security procedures necessary to ensure that compliance with responsibilities under data protection legislation and agency-specific security requirements.
- Describe how this arrangement will be monitored and reviewed.
- To illustrate the flow of information from referral through processing and outcome.

Parties to this agreement cannot amend or add appendices unless agreed as part of a formal review. It is expected that each party will have procedures, processes and policies sitting underneath this agreement, for their respective organisations. These will, for example, describe the specific processes for secure transfer of data.

1.1. Responsibilities of parties involved

The parties are registered Data Controllers under the Data Protection Act. A list of signatories is at Appendix A. All parties confirm that they comply with data protection legislation by:

- having a lawful basis for processing and sharing personal data.
- ensuring data quality.
- storing and sharing information securely, with access management controls.
- having policies and procedures for compliance with data protection legislation including for managing data subject rights and complaints, identifying and managing data breaches/incidents and retention & disposal.
- ensuring that mandatory training is undertaken regularly by their employees to ensure they are clear and up to date on their responsibilities. Every individual must uphold the principles of this agreement and overarching confidentiality and seek advice from the relevant Data Protection Officer when necessary.

- undertaking appropriate data protection due diligence checks with any contractors/data processors they employ and ensuring that a written agreement is in place with each data processor, and that all data processors will be bound by this agreement.
- having written processes for the processing of data to ensure employees use and share personal data in line with data protection law, the data protection principles, and this agreement.

Organisations and their staff must consult the organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian if they are unsure at any point in the processing and sharing of personal data.

1.2. Confidentiality and vetting

Each Partner must ensure that there are appropriate written contracts or agreements with employees, agency staff, volunteers etc. These must include requirements to ensure compliance with policies which include confidentiality. Each Partner must ensure that suitable vetting has taken place. This may be through standard employee checks and DBS checks.

1.3. Assessment and review

A review of this information sharing agreement will take place yearly, unless otherwise agreed by the organisations' Data Protection Officers. The aim of the review will be to ensure the purposes are still relevant, the scope has not slipped, the benefits to the data subjects and organisations are being realised, and the procedures followed for information security are effective.

Changes in legislation and developments in the areas of public sector data sharing will be considered as and when they arise, as will any changes to the signatory parties.

1.4. Period of Agreement and Termination of agreement

This DSA will continue indefinitely. Parties may exit the agreement if underlying contracts expire or are terminated, or if the Party's DPO gives one calendar month's written notice of their termination to the other Party's DPOs. In the event of termination of this agreement each party may continue to hold information originating from other parties for which they are Data Controller.

2. Purpose and Benefits

2.1. Purpose

This agreement covers the sharing of information by and between the listed parties for the purpose of the offering evidence based 'individual placement and support' (IPS) to people who use secondary mental health and NHS Talking Therapies services in Camden with the aim of securing and retaining paid employment. The Council has entered into a 2-year contract with Hestia Housing and Support (HHS) to deliver the IPS service, which runs for two years, 5th May 2025 to 31 March 2027. Hestia Housing and Support (HHS) will employ employment specialists and advisers who will be embedded in the clinical teams run by the North London Foundation NHS Trust (NLFT). All staff will use NLFT's data and data management/ records systems, i.e. Rio in secondary care community mental health teams and IAPTUS in ICOPE, to record their interventions or the support offered.

Staff employed by NLFT would be responsible for referring patient/clients from their caseloads to the EAs for employment support. However, people known to the NLFT teams can also self-refer. The referral

information would consist of personal and sensitive data including relevant health needs and risk management issues that might impact on the individual's ability to work.

2.2. Benefits

The sharing will allow all partners to better deliver their statutory and contractual responsibilities and will allow more effective use of resources, giving more joined up working which increases efficiency.

The public will benefit from this approach, as services will be delivered in a more streamlined way that utilises the information shared to provide better tailored and appropriate services.

Clients will receive intensive personalised support including but not limited to vocational profiling, CV writing, preparing for interviews, rapid job search followed by time unlimited in-work support for those using secondary mental health services and limited in-work support for others. Support will also be provided to the employer so that reasonable adjustment could be made and work opportunities sustained.

There is strong evidence of the benefit of work enabling people with mental health conditions to recover, which in turn reduces their use or need for health and care services. In addition, access to paid employment would promote the impendence and choice of beneficiaries.

Furthermore, the service offer aligns with the council's equity and inclusion goals by supporting individuals with mental health challenges, who are often marginalised in the labour market to achieve meaningful employment, thereby fostering a more equitable Camden.

The benefits of this DSA are to:

- Cover the sharing of information for the offer of IPS employment support to people using secondary mental health and NHS Talking Therapies services in Camden
- Sets parameters for sharing personal data and clearly identifies the responsibilities of organisations.
- Identify the correct lawful basis to share personal information.
- Ensure information is shared whenever there is a requirement to do so.
- Enables authorities to share data on performance, quality assurance, learning and impact analysis.

2.3. Lawful Basis

The sharing of information must comply with the law relating to confidentiality, data protection and human rights. Having a legitimate purpose for sharing information is an important part of meeting those legal requirements. This is a complex area and each Partner must take their own decisions and seek advice from their organisation's Data Protection Officer/Information Governance Manager and/or Caldicott Guardian.

Articles 6, 9 and 10 of the UK GDPR, and section 8 of the DPA 2018 set out the acceptable conditions for the processing and sharing of personal, special category, and criminal data. The conditions relevant in the UK GDPR to data processed under this agreement are below.

For all parties:

Personal Data : Article 6 (1) – (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Special Category Data : Article 9 (2) (b) social protection law - processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;

9 (2) (g) substantial public interest - processing is necessary for reasons of substantial public interest with the Data Protection Act Schedule 1, Part 2 condition is being para 6 Statutory etc., and government purposes

The underpinning laws are Children Acts, Care Act, Health and Safety at Work etc Act 1974; Care Act 2014; Health & Care Act 2023.

Criminal Offence Data: article 10 is met by the art 6 conditions as for personal data, and the DPA18 schedule conditions as for art 9 for special category data

2.4. Consent

The parties will often work collaboratively with data subjects and aim for agreement with them on the actions to be taken. However, it is recognised that this is different to using consent (Article 6 (a)) or explicit consent (Article 9 (a)) as the lawful basis conditions used for processing under this agreement.

Consent is not generally the lawful basis the public sector organisations use for processing information shared under this agreement. It is noted that where consent is not the lawful basis for processing, consent does not need to be sought to share, and thus the concept of “overriding consent” is a misconception.

2.5. Proportionality and necessity

Proportionality, data minimization, necessity and not being excessive are factors to be taken into consideration when deciding whether to share personal information. In making the decision, employees must weigh up what might happen as a result of the information being shared against what might happen if it is not, and apply their professional judgement. It is for this reason professionals must ensure they comply with Article 5(1)(c) and share the adequate and relevant information, and limit that information to what is necessary for the achieving of the DSA aims.

2.6. Freedom of Information

The Freedom of Information Act 2000 gives all individuals the right to access official information held by a public authority (the Environmental Information Regulations 2004 also allow access to data. For ease of drafting, FOI is used to cover both legislation). Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature.

All requests for FOI will be directed through the relevant organisations’ FOI processes. Each party will seek advice/opinion from the other parties where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the party who received the request as the legal duty lies with them. In order to ensure that the authority in receipt of the

FOIA request is able to respond within the statutory deadline, any request for assistance or information made to partner authorities should be made and processed within two working days, and any data exchange completed within seven working days. It is encouraged that all parties proactively publish this document. It may also be disclosed to the public under FOI.

3. Individuals

Organisations processing personal data are required to begin with the ethos of Data Protection by Design and Default (also known as Privacy by Design (PbD)). This means that we must consider and uphold the privacy of an individual's data before we begin and throughout the processing taking place.

Each party agrees that they have undertaken a DPIA (Data Protection Impact Assessment), where they feel the processing meets the legislative criteria for a DPIA.

3.1. Right to be informed – Privacy notices

Where personal data is created or received by one of the parties, they are responsible, as required by law, for making the data subject(s) aware within a reasonable time frame that the organisation holds the data, what they will do with it, how long they will keep it, and who they will share it with (such as under this DSA). This is normally done through a privacy notice, whether written or verbal. Organisations agree that they will adhere to the transparency requirements of the UK GDPR and will issue appropriate notices which inform the data subject that the information will be shared with the parties under this agreement. In some cases, it may not be appropriate to let a person know that information about them is being processed and shared. Consideration should be given to whether notifying the individual may place someone at risk or prejudice a police or safeguarding investigation. In these circumstances, the parties need not inform individuals that the information is being processed/shared; but should record their reasons for sharing information without making the individual aware.

3.2. Data subject rights requests and complaints

Each organisation must have in place appropriate policies and processes to handle data subject requests made in line with data protection law, to ensure they are responded to within deadline and in an appropriate manner. Requests include; right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision making including profiling.

If an individual successfully requests the erasure or limitation of use of their data (right to erasure, right to rectification, right to restrict processing, right to object), the party that has been informed by the data subject will communicate this to the other parties where relevant and appropriate. In each case each party is responsible for securely disposing of such information or limiting its processing.

Each party must have clear, fair and objective complaint procedures. Any complaints from individuals how their data is being processed or shared will be handled under the policy and processes of the organisation concerned.

3.3. Data subjects

The data subjects will be people who are known to and supported by clinicians in secondary mental health and NHS Talking Therapies services/teams run by the Camden Division of the NLFT as well as

mental health adult social care staff in aligned neighbourhood teams. They could be referred to the IPS Employment services by members of the said teams, themselves and their care/support network

4. Data

4.1. The data to be shared

Data that will be shared includes:

- name
- Postal and email addresses
- Telephone/mobile number
- Gender
- National Insurance Number
- age/date of birth
- Sexual orientation
- Ethnicity
- Physical and mental health needs including any reasonable adjustment and/or in work support the client may need
- Financial information including welfare benefit
- Education history
- Employment status including details of current employer if in employment
- Information on employment history and aspiration
- Start (and/or end) date of employment.

4.2. Storing and handling information securely

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system.

All parties will have access and able to use NLFT's data and data management/ records systems, i.e. Rio in secondary care community mental health teams and IAPTUS in ICOPE, to record interventions or the support offered.

All laptops, computers, and any other portable devices will be encrypted. Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer. There is an expectation that partner organisations will either

be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security.

Unencrypted email (i.e. sent in plain text over the public internet) must not be used to share information under this DSA.

Sharing methods that may be appropriate include:

- **Email encryption tools** where the email and attachments are encrypted from named sender to named recipient (e.g. Microsoft 365 Message Encryption; Egress Protect)
- **Encryption via Transport Layer Security** (TLS) where the email and attachments are encrypted in transit over the internet. Both the sender and recipient email domains must have TLS enabled. This can be checked using https://www.checktls.com/
- **Secure corporately managed data repository and sharing platforms** (e.g. MS Teams; Google Docs)
- **Secure group email services** (e.g. NHS Mail- NHSmail 2 Portal - Home)
- **Secure File Transfer Protocols**
- **Virtual Private Networks**

The above are examples, Parties to this agreement should get advice from your organisation's information security or IT teams on secure methods of sharing available at your organisation and document these in the organisation's process documents.

Phone/virtual meetings/face-to-face meetings:

Information may be shared over the phone, in a virtual meeting, or at face-to-face meetings. Meeting attendance and distribution of content, e.g. meeting minutes or recordings, must be limited to those with a need to know.

Sharing by telephone should be avoided unless the requirement is urgent and email is not practicable.

Individuals should be aware of their surroundings and the presence of other individuals or voice recognition or 'Internet of Things' devices (e.g. virtual assistant apps like Alexa, Cortana, SIRI) to ensure they aren't overheard by those that should not have access to the information discussed. Use of acronyms/or reference numbers other than names are advised.

Paper records:

Printed paper records must always be kept to a minimum and kept secure whether in the office, home or during transit. Organisations must adopt an appropriate policy surrounding the use and transfer of paper records. Appropriate security methods must be applied when storing or disposing of paper records.

4.3. Access controls and security

All parties will ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

All personal data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The systems will be auditable so that it is possible for any auditor to establish who has accessed the system. All parties will have access and able to use NLFT's data and data management/ records systems, i.e. Rio in secondary care community

mental health teams and IAPTUS in ICOPE, to record interventions or the support offered. All laptops, computers, and any other portable devices will be encrypted.

Any individual no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

There is an expectation that partner organisations will either be working toward ISO 27001, the International Standard for Information Security Management, or a similar standard of security such as NHS Digital's Data Security and Protection Toolkit (DSP) and Cyber Essentials or Cyber Essentials Plus.

4.4. Outside UK processing

Parties are responsible for ensuring that if information is processed or shared outside the UK, that appropriate safeguards are in place and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. These are for example, a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, and/or standard data protection contractual clauses.

4.5. Data quality

Each partner is responsible for ensuring the accuracy and relevance of the personal data that it processes and shares and must have clear processes in place for managing data quality.

Any party learning of the inaccuracy of personal data is responsible for informing the parties with whom that data has been shared.

4.6. Data breaches/incidents

All parties must have a clear policy and procedure regarding the reporting and handling of data protection breaches or data loss incidents. This must include assessing the level of risk to the data subject(s), as well as to make a decision on notifying the ICO within the statutory time frame of 72 hours. This complies with Articles 33 and 34 of UK GDPR.

If the incident may impact the processing of another party to this agreement, all relevant parties should be informed and appropriate coordination of the incident must take place. The decision to report the incident will lie with the data controller(s) of the information concerned. The parties agree to provide all reasonable and necessary assistance at their own expense to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.

It is confirmed that security breaches (including misuse or unauthorised disclosure) are covered by the partner's internal disciplinary procedures. If misuse is found there should be a mechanism to facilitate an investigation, including initiating criminal proceedings where necessary.

4.7. Retention and Disposal

Organisations are required by data protection legislation to document processing activities for personal data, such as what personal data is held, where it came from and with whom it has been shared. This Record of Processing Activity (ROPA) must include the retention period for the data.

Information must not be retained for longer than necessary for the purpose for which it was obtained. Disposal or deletion of personal data once it is no longer required, must be done securely with appropriate safeguards, in accordance with that organisation's disposal policies.

5. Signatures

For London Borough of Camden	
Name	[redacted]
Designation/Role	Head of Service – Mental Health, Learning Disabilities & Autism
Signature	[redacted]
Date	02/05/2025

For North London NHS Foundation Trust	
Name	[redacted]
Designation/Role	Managing Director
Signature	[redacted]
Date	02/05/2025

Version control	
Document production date	04 Feb 2025

Version control	
Document currency	DSA-CAM MH IPS Emp Services- 040225

6. Appendices

6.1. Appendix A: Parties to this agreement

Organisation	Duties
London Borough of Camden	• To monitor compliance with the contract and delivery of the commissioned service, officers will review anonymised data provided by Hestia Housing and Support.
North London Foundation Trust	• NLFT to process data and send via the referral information to Hestia Housing and Support. It would be used to develop a support plan focussed on securing paid employment for the individual. Data will come from NLFT systems RIO and IAPTUS • NLFT has a dedicated data management role to undertake data quality checks to ensure that data being process is accurate and of high quality
	•