



NORTH LONDON PARTNERS
in health and care

North Central London's sustainability
and transformation partnership



NORTH LONDON HEALTH AND CARE PARTNERS

PRIVACY NOTICE



We are working across Barnet, Camden, Enfield, Islington and Haringey to join up health and care records.

NORTH LONDON HEALTH AND CARE PARTNERS - HEALTH INFORMATION EXCHANGE (HIE) SYSTEM

PRIVACY NOTICE - last updated 01/12/2020

1.0 Introduction

The data protection regulations in the UK include the Data Protection Act 2018, the “Applied General Data Protection Regulation” created by that act, and the Privacy and Electronic Communication Regulations 2003. From 1 Jan 2021, the UK Data Protection Act will apply, amended from the EU act by relevant Brexit regulations. The EU GDPR 2016/EU679 will still apply to the processing of data relating to persons resident in the EEA.

A requirement of the data protection regulations is that we inform individuals about whom we hold data (data subjects) about our processing (GDPR Articles 13/14). A Privacy Notice is information given to ensure you (the data subject) are aware of how your data is being used or shared.

This notice details the following:

- What information we collect and hold about you
- The legal basis for collecting and holding the information
- What we do with it, how we keep it secure (confidential)
- Who we might share it with
- How long we will hold it for
- What your rights are in relation to your data.

2.0 Who we are

This privacy notice is issued by the North Central London CCG acting on behalf of the North London Partners in Health and Care.

The North London Partners in Health & Care (NLP) are a partnership of local authorities and health and care organisations from Barnet, Camden, Enfield, Haringey and Islington. We are working together to improve health and wellbeing outcomes for our population of 1.5 million people.

The partners are signatories to a Data Sharing Agreement which demonstrates a robust foundation for the lawful, secure and confidential sharing of personal information between themselves.

Each partner organisation has appointed a Data Protection Officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. Each partner is controller of the data that it accesses via these systems and responsible for processing that data in line with data protection regulations.

NLP are not the data controller of your information – this is the partner organisations, as listed in Appendix A. Generally, the controller of your information will be the organisation(s) providing your care e.g. your GP, your hospital, your local authority. This notice covers specific systems for which NLP is the processor.

This privacy notice contains information about the processing of Personal Information by North London Health and Care Partners using the following systems:

- Health Information Exchange (HIE)
- HealthIntent (HEI)

3.0 Health Information Exchange (HIE) System

A record of care is held on each partner's secure clinical system (local record). Cerner, a supplier of healthcare systems has designed HIE. This system integrates data from those multiple electronic health and care systems to provide a real-time and read-only summary of that data to a health or social care professional when required for the purpose of your direct care.

The care provider can see relevant parts of your clinical record; this excludes certain sensitive data items as detailed below and is role-based – for example a doctor sees different information to a health care assistant or a social worker. Each role sees only information relevant to their direct care to you.

4.0 HealthIntent (HEI) system

HealthIntent is a platform that will allow health and care professionals in North Central London to be more proactive in the care of patients and communities.

The system links elements of health and care information from different sources and enables clinicians to manage and plan care for individuals and groups of residents in relation to health or social care. Health care professionals directly involved in a patient's care can view a patient's joined-up record, showing information collected by different providers over time. The joined-up record helps to spot trends, concerns or gaps in care. This information contained in this record is used to create 'registries' and 'analytics'.

- **Registries** give a dashboard view to show how one or more patients are doing relating to agreed measures associated with particular conditions. For example, the diabetes dashboard shows measures relating to the effective management of care for a patient, or groups of patients with diabetes, such as BMI, or regular eye and foot exams. The dashboard will present up-to-date relevant information, from all care providers, and alert clinicians to any gaps or duplication.



- **Analytics** can help to spot trends and variation in groups of patients and help professionals to identify any specific actions that need to be taken to improve care.
- **Dashboards** will be available to support case finding for individual patients.

5.0 The purpose(s) of the sharing

HIE and HEI are Electronic Health Record (EHR) linking systems that bring together patient/client information across health and care systems in a secure manner, giving a real-time summary of your information which is held within a number of local records/systems. The sharing of health information is a requirement placed on Health and Social Care Providers by the Health and Social Care Act.

Most data on HealthIntent (HEI) will be anonymised. Only a healthcare professional who is directly involved in a patient's care will be able to see that individual patient's record.

Benefits of these systems are;

- Improved quality of care – information about your care will be instantly available to clinicians for more accurate diagnosis and on-going treatment. Duplication of tests will be avoided.
- Improved patient safety – there will be greater visibility for your health and social providers about your current medications, allergies and adverse reactions.
- Reduced delays in care – test results will be readily available reduces patient waiting time.

6.0 The categories of personal information we share

Personal information (or Personal Data) means any information about individual from which that person can be identified. It does not include information where the identity has been removed (anonymous data). The Personal Data that is shared includes:

Identifying Data: Forename, Surname, Address, Date of Birth, Gender, Age, Postal Address, Postcode, Telephone Number, NHS Number and Hospital ID

Special categories of Personal Data: Racial or ethnic origin, Physical/mental health or condition. For example, blood test results, MRI scan results, etc.

However, not every element of your information is part of the joint record. Examples of the sensitive information that will be left out include fertility treatment records, domestic violence and criminal records.

7.0 What is the lawful basis for the sharing?





Under the data protection regulations the processing of personal data for the purpose of health and social care provision is permitted by the Data Protection Act 2018 section 8(c) – “the exercise of a function conferred on a person by an enactment or rule of law”, specifically the NHS Act 2006 and the Health and Social Care Act 2012. The processing (sharing) of Personal Data for these purposes is permitted under Article 6(1) (e) of the General Data Protection Regulation:

Public Task: the 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

For special category personal data (including health data), the processing (sharing) is permitted under the Data Protection Act section 10 (1) (c) – health and social care via Schedule 1 Part 1 section 2 “Health or social care purposes” satisfying section 10 (2) of permitting the legal basis of Article 9 (2) (h) of the General Data Protection Regulation:

Direct Care and Administration: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

We will also recognise your rights established under UK case law collectively known as the “Common Law Duty of Confidentiality”

8.0 What we use your Personal Data and special categories of Personal Data (known as or sensitive personal) for

The Personal Data that we share will be used by the partners to provide you with the best possible direct care delivery.

9.0 Organisations we share your personal information with

The data will be shared with health and social care professionals providing direct medical care to you (the data subject), with a legitimate relationship to you as a patient. This includes organisations outside of North London Partners where you are receiving treatment or services from them.

10.0 How will the information be made available?

The information is accessed in real time and on-demand and presented as a read only view; meaning that the Personal Data from a partner's local record is not changed. The data remains within each Partner's database and users are allowed read-view access only. Access to your data depends on the professional having



access in their own clinical systems, so professionals can only see information regarding patients that are being referred for treatment or have been treated by them.

11.0 How long do we keep your record?

Both HIE and HEI are only used to share, rather than store, data contained within a local record, the retention of data is set by individual partners who follow the NHS Records Management Code of Practice for Health and Social Care 2016 and the NHS Record Retention Guidelines.

12.0 How we keep your personal information safe and secure

We ensure the information we hold is kept in secure locations and access is restricted to authorised staff only. All staff are obliged to always keep the information secure and confidential at all times and not share it with other colleagues without proper authorisation.

Our appropriate technical and security measures include:

- Complying with Data Protection regulations
- Encryption of all Personal Data transmitted between partners
- Encryption of all Personal data stored on the systems and databases in partner organisations
- Implementing and maintaining business continuity and disaster recovery plans, relevant policies and procedures
- Completion of the Data Security and Protection Toolkit (DSPT) on an annual basis to evidence compliance with all the information governance management and accountability arrangements
- Use of 'user access authentication' mechanisms to ensure that all instances of access to any Authority Personal Data under both the HIE and HEI systems are auditable against an individual
- Ensuring that all employees and contractors who are involved in the processing of Personal Data are suitably trained in maintaining the privacy and security of the Personal Data and are under contractual or statutory obligations of confidentiality concerning the Personal Data.

The NHS Digital Code of Practice on Confidential Information applies to all of our staff, and they are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. All staff with access to Personal Data are trained to ensure information is always kept confidential.

13.0 What are your rights?

Under the Data Protection regulations, you have the right to:

- Be informed of our uses of your data (the purpose of this document)



- Request copies of your personal information and to use these for data portability
- Request rectification of any inaccuracy in your Personal Data or special categories of Personal Data
- Restrict the processing of your personal information where the accuracy of the data is contested or, where the processing/sharing is no longer needed
- Not be subject to automated decision making or profiling. There is no automated decision making or profiling in HIE
- Complain about our handling of your data to our data protection officer or to the regulator
- You also have the right to opt out of sharing Personal Confidential Data via HIE (the right to object to processing).

Details of how to exercise your rights are given in this document.

14.0 How can I access the information you keep about me?

To access your Personal Data, you should contact the appropriate partner (Appendix A).

If this data contains errors, you can exercise your right to correct this by contacting the partner's Data Protection Officer.

15.0 How can I “opt-out” of data sharing via HIE?

We ask you to think carefully before making this decision as sharing your health and social care information **will make it easier for services to provide the best treatment and care for you.**

If you chose to opt-out, we may still need to share data for your care, but it will be using less immediate methods such as email. For example, with HIE, your GP can refer you to a hospital consultant who can then see all the data they may need, but if you are opted-out they can only see what the GP put on the email.

If you would like to speak to someone about your choice, you can call our enquiry line on **020 3688 1900**.

You can opt-out of having your Personal Data shared via HIE by completing the attached form and return it to us or by using the form on our website.

<http://www.northlondonpartners.org.uk/downloads/plans/Digital/NLP%20Resident%20Leaflet%20English%20OPT%20OUT%20FORM.pdf>

Before opting out, **please ensure that you have read the Health Information Exchange Opt-Out leaflet carefully** and understand what it means for you. If you choose to opt-out:

- You may have to answer questions repeatedly because your full history may not be available to the care professional assessing you.
- Decisions about your care may take longer, even in emergency situations, as history needs to be confirmed.





- Some medical tests may get repeated unnecessarily e.g. if you had a blood test with your hospital consultant, your GP may not be able to see this.

16.0 Right to complain

You can get further advice or report a concern directly to:

- NCL CCG Communications Team
- A relevant partner (listed on Appendix A), or
- The UK's supervisory authority (Information Commissioner's Office) by:

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Telephone: 0303 123 1113 (local rate) or 01625 545745 (national rate)

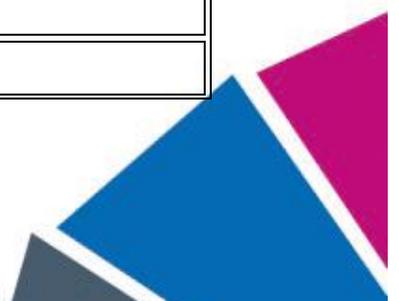
Email: <https://ico.org.uk/concerns/handling/>





Appendix A List of Partners

Partners
Barnet Enfield and Haringey Mental Health NHS Trust (main sites, incl. Enfield Community)
Barnet Federation
Barnet GPs
Camden and Islington NHS FT (and main sites)
Camden GP Federation
Camden GPs
Central and North West London NHS FT (Camden Community)
Central London Community Healthcare NHS Trust
Enfield Federation
Enfield GPs
Great Ormond Street Hospital
Haringey Federation
Haringey GPs
Islington Federation
Islington GPs
London Borough of Barnet
London Borough of Camden
London Borough of Enfield
London Borough of Haringey
London Borough of Islington
Marie Curie
Moorfields Eye Hospital NHS Foundation Trust
North Central London Clinical Commissioning Group
North London Hospice
North Middlesex University Hospital NHS Trust
Royal Free London NHS Hospitals Foundation Trust
Royal National Orthopaedic Hospital NHS Trust
Tavistock and Portman NHS Foundation Trust





Partners

University College London Hospitals NHS Foundation Trust.

Whittington Health NHS Trust

Version	Review by	Date	Outcome
0.1	IG Sub-Group	07 February 2019	Approved with minor changes
0.2	NLP IG Group	27 February 2019	Changes requested for clarity
0.3	NLP IG Group	1 December 2020	Revised Notice to include HIE and HEI processing

