**Practice Privacy Notice**

**Contents**

[1. Introduction 2](#_Toc516064652)

[2. What is this Privacy Notice about? 2](#_Toc516064653)

[3. Who we are 2](#_Toc516064654)

[4. Types of information we use 2](#_Toc516064655)

[5. What we use your personal data and special categories of personal data (known as or sensitive personal) for 3](#_Toc516064656)

[6. Identity and Contact details of the Data Controller and Data Protection Officer 3](#_Toc516064657)

[7. Organisations we share your personal information with 3](#_Toc516064658)

[8. What is EMIS Systems Local Record Sharing? 3](#_Toc516064659)

[9. What do we use anonymised data for? 4](#_Toc516064660)

[10. Details of data linkage with other datasets 4](#_Toc516064661)

[11. What safeguards are in place to ensure data that identifies me is secure? 4](#_Toc516064662)

[12. What are your rights? 5](#_Toc516064663)

[13. Gaining access to the data we hold about you 5](#_Toc516064664)

[14. What is the right to know? 5](#_Toc516064665)

[a. What sort of information can I request? 5](#_Toc516064666)

[b. How do I make a request for information? 6](#_Toc516064667)

[15. Glossary of Terms 6](#_Toc516064668)

# Introduction

The UK Data Protection Bill will become law when enacted as the Data Protection Act 2018. It will explicitly bring provisions of the EU General Data Protection Regulation (GDRP) 2016 into UK law and establish continuity of the GDPR. The Act will legislate in areas where the GDPR allows flexibility at national level. It will also introduce legislation on processing for law enforcement purposes (in support of the EU Law Enforcement Directive) and by the intelligence services, and make provision for the Information Commissioner (the UK supervisory authority). The current Data Protection Act (DPA) 1998 will be completely repealed when DPA 2018 comes in force.

This Privacy Notice has been written in line with the EU GDPR 2016. The Privacy Notice will be reviewed when the DPA 2018 comes in force in order to align it with the Act.

# What is this Privacy Notice about?

Privacy Notice is the conditions which have to be met for any activity involving personal data or special categories of personal data to be lawful. Being transparent and providing accessible information to individuals about how an organisation will use their personal information is a key element of Data Protection Legislations. The most common way to provide this information is in a Privacy Notice.

This Privacy Notice is part of our programme to make the data processing activities we are carrying out in order to meet our healthcare obligations transparent.

The Privacy Notice tells you about 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 and what your rights are in relation to your information.

# Who we are

Colindale Medical Centre provide General Practice services as part of the PMS (Personal Medical Services) contract we hold with NHS England. The practice sits within the Barnet Clinical Commissioning Group (CCG).

The practice consists of 2 GP Partners, Dr Manu Lamba and Dr Amrit Lamba, supported by a Practice Manager, a team of GPs, nurses, clinical pharmacists, and an administration and reception team. The practice provides general practice care to its registered patients living within the Colindale NW9 area.

Colindale Medical Centre may be referred to as ‘we’, ‘us’, ‘the practice’, ‘the surgery’.

# Types of information we use

We use the following types of information/data:

* Personal data or sensitive personal/special categories of personal data such as:
* demographics – name, address, date of birth, postcode, NHS number
* racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, medical/health data, sexual life or sexual orientation data.
* Pseudonymised - about individuals but with identifying details (such as name or NHS number) replaced with a unique code.
* Anonymised - about individuals but with identifying details removed.
* Aggregated - anonymised information grouped together so that it doesn't identify individuals.

# What we use your personal data and special categories of personal data (known as or sensitive personal) for

We use and share information about you in a number of ways. These include:

***Primary uses -*** information from your GP medical record which can be made available to other NHS and public sector organisations, including doctors, nurses and care professionals in order to help them make the best informed decision, and provide you with the best possible direct care delivery.

***Secondary uses -*** information from your GP medical record involves extracting identifiable data and (usually) sharing that data with other NHS organisations, for the purpose of indirect care. Examples include using your information for [research](https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/), auditing, and healthcare planning (population health management).

# Identity and Contact details of the Data Controller and Data Protection Officer

Data Controller: Dr Amrit Lamba, Colindale Medical Centre, 61 Colindeep Lane, London NW9 6DJ

The Data Protection Officer (DPO) is:

Steve Durbin, Data Protection Officer, Barnet GP Federation

Email: barnet.federation@nhs.net

Postal: 234 Burnt Oak Broadway, Edgware, HA8 0AP

# Organisations we share your personal information with

We share information about you with other GPs, NHS acute or mental health Trusts, local authority, community health providers, pharmacists, commissioning organisations, medical research organisations and some specific non NHS organisations for the purposes of direct and indirect care delivery of care.

We also share information with HIE (Health Information Exchange). HIE is an electronic Health Record (HER) linking system that brings together patient/client’s 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. The HIE’s privacy statement can be found at:

<http://www.northlondonpartners.org.uk/downloads/plans/Digital/Privacy%20Notice%20version%2002.pdf>

The legal basis for processing personal data is a Legal obligation and/or is necessary in order to protect the vital interests of the data subject. Special Category data is processed in the field of employment, social security and social protection law and/or is necessary for medical or social care treatment or, the management of health or social care systems and services.

Data is retained in line with the [Records Management Codes of Practice for Health and Social Care](https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care).

Further details can be found in [Appendix A Processing of Data](file:///C%3A%5CUsers%5Cemis2000%5CDownloads%5CAppendix%20A%20Processing%20of%20Data.rtf).

# What is EMIS Systems Local Record Sharing?

Your GP medical record is held on our secure clinical system called EMIS Web. This clinical system allows for local record sharing with other healthcare providers who are commissioned in your area to provide care (e.g. acute hospitals, mental and community health). Through this record sharing, clinicians are able to see clinical information entered by other organisations who are party to the EMIS local record sharing agreement.

This local sharing is used to provide direct patient care for services such as continued extended access, home visits, universal offers, musculoskeletal service, GP at front door and other neighbourhood services across Barnet in line the local Care delivery strategy and the NHS STP.

It also enables specific GPs identify their patients with highly complex, multiple morbidity and/or frailty, who might benefit from targeted multi-disciplinary team support as part of case management and care planning (the "Case Finding Purpose").

**How will my information be made available?**

The information is accessed in real time and on-demand, meaning that data from your GP record is neither extracted, nor uploaded, nor sent anywhere. The data remains within your GP EMIS database and users are allowed read-view access only. If you have any concerns regarding EMIS local record sharing you can opt out by speaking to your GP Surgery.

# What do we use anonymised data for?

We use anonymised data to plan health care services. Specifically we use it to:

* check the quality and efficiency of the health services we provide;
* prepare performance reports on the services we provide and,
* review the healthcare we provide in order they are of the highest standard.

# Details of data linkage with other datasets

Data may be de-identified and linked so that it can be used to improve health care and development and monitor NHS performance. Where data is used for these statistical purposes, stringent measures are taken to ensure individual patients cannot be identified.

When analysing current health services and proposals for developing future services it is sometimes necessary to link separate individual datasets to be able to produce a comprehensive evaluation.  This may involve linking primary care GP data with other data such as secondary uses service (SUS) data (inpatient, outpatient and A&E).  In some cases there may also be a need to link local datasets which could include a range of acute-based services such as radiology, physiotherapy, audiology etc, as well as mental health and community-based services such as ‘Mind Matters’ (Psychological Therapies), community nursing, podiatry etc.  When carrying out this analysis, the linkage of these datasets is always done using a unique identifier that does not reveal a person’s identity.

The organisation responsible for processing de-identified and linked data under this category, on behalf of the Practice is Barnet CCG (Clinical Commissioning Group). We ensure that the data processor is legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed.

# What safeguards are in place to ensure data that identifies me is secure?

We only use information that may identify you in accordance with the EU General Data Protection Regulation 2016. These Legislation requires us to process personal data only if there is a lawful basis for doing so and that any processing must be fair and lawful.

We also ensure the information we hold is kept in secure locations, restrict access to information to authorised personnel only, protect personal and confidential information held on equipment such as laptops with encryption (which masks data so that unauthorised users cannot see or make sense of it).

Our appropriate technical and security measures include:

* The ability to ensure ongoing confidentiality, integrity, availability and resilience of our systems;
* the ability to quickly restore availability and access to personal information in the event of a physical or technical incident; and
* a process regularly testing, assessing and evaluating the effectiveness of security measures, and ensure they comply with the concept of privacy by design and default.

The [NHS Digital Code of Practice on Confidential Information](http://systems.digital.nhs.uk/infogov/codes) 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 Practice staff are trained to ensure information is kept confidential.

We are registered with the Information Commissioner’s Office (ICO) as a data controller and collects data for a variety of purposes. A copy of the registration is available through the [**ICO website**](https://ico.org.uk/esdwebpages/search). You can search by our Practice name: Colindale Medical Centre or ICO Data Protection Register number **Z5297703.**

# What are your rights?

Where information from which you can be identified is held, you have the:

* Right of access to view or request copies of the records
* Right to rectification of inaccurate personal data or special categories of personal data
* Right to restriction of the processing of your data where accuracy of the data is contested, processing is unlawful or where we no longer need the data for the purposes of the processing
* Right to object to any automated individual decision-making
* Right to data portability by requesting the data which you provided to us (not data generated by us) in a structured, commonly used machine readable format. Your right to portability applies only where:
* data is processed by automated means, and
* you provided consent to the processing or,
* the processing is necessary for the fulfilment of a contract

These rights will only apply where we cannot demonstrate compelling legitimate grounds for continued processing of your personal data for the purposes of direct provision of care, and compliance with a legal obligation to which we are subject.

**Your right to erasure (right to be forgotten)** will only apply where you had given ‘consent’ to process your personal health data and later withdrew the consent, **and does not apply to the extent** where the processing of your personal health data is necessary for:

* [Compliance with a legal obligation which we are subject to, under the UK law or, for the performance of a task carried out in the public interest or, in the exercise of official authority vested on us;](https://gdpr-info.eu/art-6-gdpr/)
* [medical purposes and/or for reasons of public interest in the area of public health](https://gdpr-info.eu/art-9-gdpr/);

[archiving purposes in the public interest, scientific or historical research purposes or statistical purposes](https://gdpr-info.eu/art-17-gdpr/);

[the establishment, exercise or defence of legal claims](https://gdpr-info.eu/art-17-gdpr/)

You can exercise your rights at any time bycontacting the Practice (data controller) or the Data Protection Officer (DPO) at the address below, although we will first need to explain how this may affect the care you receive and any overriding legitimate grounds for the processing that may apply.

# Gaining access to the data we hold about you

You have the right to see or have a copy of personal data we hold that can identify you. You do not need to give a reason to see your data. However, some information may be withheld under some exceptional circumstances.

If you want to access your personal information you must do so in writing by **completing our** Subject Access Request (SAR) form [insert link] send it to:

Subject Access Requests

Colindale Medical Centre

61 Colindeep Lane

London NW9 6DJ

# What is the right to know?

The Freedom of Information Act 2000 (FOIA) gives people a general right of access to information held by or on behalf of public authorities, promoting a culture of openness and accountability across the public sector.

## What sort of information can I request?

In theory, you can request any information that the Practice holds that does not fall under an exemption under the FOI Act. You may not ask for information that is covered by the Data Protection Act or EU General Data Protection Regulation (GDPR) under FOIA. However, you can request this under a Subject Access Request – see section above ‘Gaining access to the data we hold about you’.

## How do I make a request for information?

Your request must be in writing and can be either posted or emailed to:

**Email**: colindeeplane.surgery@nhs.net

**Post:** Colindale Medical Centre, 61 Colindeep Lane, London NW9 6DJ

# Glossary of Terms

[**Common Law of Duty of Confidentiality**](https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality)- is not written out in one document like the GDPR or an Act of Parliament. Common Law is also referred to as ‘judge-made’ or case law. In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client. However, where the disclosure/sharing of the patient/client information is for the purpose of Direct Care consent to such disclosure/sharing may be implied where it is informed, given there is a legitimate relationship between the patient/client and the health professional.

**Personal Data -** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Special Categories of Personal Data –** data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.