Introduction

We are Patient Care Locally ("PCL," "us," "we," "our"), Registered in England and Wales, registration number: 07789175.

We are registered with the UK supervisory authority, the Information Commissioner's Office ("ICO") in relation to our processing of Personal Data under the registration number: ZA018698.

We are the data controller for the information we hold about you. A data controller is the organisation that makes decisions about the personal data that is being collected and processed, and we are ultimately in charge of and responsible for the processing.

You can contact us in relation to this notice and raise any queries about it and / or exercise your right to access your information using the details below:

Address: Office 2 and 3, Coalville Business Centre, Goliath Way, Coalville, Leicestershire LE67 3FT

Phone: 0116 380 0590

Email: pcl.datagovernance@nhs.net

PCL has been commissioned to provide healthcare services on behalf of GPs and the Integrated Care Board (ICB) through our Referral Support Service (RSS) and local provider healthcare sites. Healthcare providers screen referrals and direct the patient to the most appropriate clinical setting where they are treated either by local provision community sites contracted via PCL or in an acute hospital setting. We use a clinical system called TPP SystmOne like other healthcare providers to securely record your healthcare information.

At PCL we are committed to protecting and respecting your privacy, informing you of your rights under the Data Protection legislation and giving you access to these rights.

This Privacy Notice sets out important details about how PCL and its staff are responsible for your information, what we may collect and hold about you, how that information may be used and your legal rights.

We will review this Privacy Notice on a regular basis, and we advise you to check back on our website for the latest version.

What Information Does PCL Hold About Me?

We hold two types of personal data about you.

a) Personal Data (Data Which Identifies You)

Personal data includes information about people like their name, phone number, email address, address, date of birth, etc.

We may also hold another type of personal data, called special category data, or criminal conviction and offences data. These are more sensitive, and PCL may only process them in more limited circumstances.

Some data we hold may be pseudonymised to help reduce privacy risks by making it more difficult to identify individuals, but it still counts as personal data.

b) Special Category Data (Sensitive Data)

This sort of data could include:

Racial or ethnic origin

Political opinions

Religious or philosophical beliefs

Trade union membership

Genetic data

Biometric data (where used for identification purposes)

Health

Sex life

Sexual orientation

How Does PCL Collect Information About Me?

The information we collect and process about you has either been provided by you or by others involved in your care or treatment (e.g. GP, hospital, community, employers).

This is likely to include your personal data and more sensitive information about you especially around your health (see definitions in section 2).

We may collect information from you when:

You contact us via telephone calls which may be recorded and retained for a limited period for training and monitoring purposes and to help improve our services.

You communicate with us via email, social media, or our website.

If you book an appointment for one of our services online, we collect the details you give us, such as your name, contact details, date of birth and appointment preferences. We use this to arrange your appointment and send you confirmations and reminders.

We interact with you as part of the referral process to ensure the information we have been provided is up to date.

We may also obtain information about you from:

Other health or care providers, such as your GP to provide you with healthcare services.

Government agencies such as HMRC.

Why PCL Use the Information It Holds About Me?

We use the information we hold about you in connection to:

Referral to the best treatment and/or care pathway

Referral for tests or assessments

For medical examinations and delivery of care pathways

For service improvement

For anonymous key performance indicator reporting in relation to contractual obligation

We may also use information about you where there is a legal or regulatory obligation on us to do so (such as the prevention of fraud or safeguarding) or in connection with legal proceedings.

We may also use information about you where you have provided your consent to us doing so.

We do not carry out automated decision making or profiling.

Who Has Access to the Information About Me?

PCL collects personal Information for your health care purposes. There may be instances where we are required under legislation to share that information, but we will only do so if we have a legal basis.

We carefully control who has access to your information. Staff only have access where they are required to do so in relation to their job role, e.g. to provide direct care or support (i.e., receptionist and secretary). Where possible we limit the access that staff have on our systems.

In order to reduce risk of a data breach PCL has in place robust policies and procedures, and we carry out training for all staff on a regular basis.

We also carry out spot checks and audits to see if there has been any inappropriate access. Where that occurs, disciplinary action may be taken against the staff. If a data breach includes access to your information, we will contact you. We also have an obligation if it is a serious data breach to inform the Information Commissioner's Office.

How Do You Keep My Information Safe and Secure?

PCL is required to complete the NHS Digital Data Security and Protection Toolkit. This is a tool that provides assurance that we are meeting standards on handling patient/client information.

We have in place Data Protection Policies and Information Security Policies to ensure staff understand the 'must' or 'must not do' with patient/client data.

Staff are required to complete induction training in Information Governance and to complete update training on a regular basis.

Spot checks are carried out across the organisation.

Our IT is managed by outsourced IT providers who ensure that all safeguards are in place on our IT systems to protect data and keep it secure from unauthorised access, loss or damage.

Passwords are changed on a regular basis, and we use multi-factor authentication across all available systems.

Where incidents do happen, our investigations include actions we take, and lessons learnt.

Will PCL Share Information About Me With Others?

Yes, we set out these reasons below and assure you that in each case, we share only such information as is appropriate, necessary, and proportionate.

Provision or delivery of care or health services: Doctors/GPs, Nurses, Pharmacists, Physiotherapists

Provision of blood and lab services: Local NHS hospitals; Independent pathology/clinical laboratory services

Emergency contact in a critical situation: Anyone you have asked us to communicate with or whose details you have provided as an emergency contact (such as your next of kin)

Recording of calls when you contact us for training and monitoring: Ring Central

Reporting of anonymised data on use of services: LLR ICB (in anonymised format)

System support and management by 3rd parties: Third party suppliers which provide us with electronic patient management systems and other information technology systems including incident management and recording systems, electronic prescribing systems and other clinical and non-clinical software applications and related services

Regulatory bodies with statutory powers to access records, and court orders: Care Quality Commission; ICO; Medicines and Healthcare products Regulatory Agency; NHS England and the Department of Health; Health & Safety Executive; Public Health England

Prevention and detection of crime or fraud: Police and other third parties; The Home Office; HMRC; NHS counter fraud authority

Third parties who provide business services to us: Our lawyers; Auditors; Insurance companies

Shared Care Record across the local region (LLR Shared Care Agreement): GP Connect API and Associated Services

If you would like more detailed information on who we share your data with, please contact us.

Artificial intelligence and automated decision-making

We may use artificial intelligence (AI) for marketing and administrative purposes. We may use artificial intelligence (AI) and other automated technologies as part of the delivery of some healthcare services. Where we do so, we will explain how the technology is used, the personal information involved and the role it plays in decisions about your care.

For example, within certain dermatology pathways, images of skin lesions and relevant clinical information may be analysed using an AI-enabled system to help assess the lesion and recommend an appropriate pathway, such as discharge or referral for further assessment. Rest assured a clinician reviews the AI output and makes or confirms the decision, the decision is not made solely by automated means. Personal identifiable information will be deidentified prior to AI analysis.

If PCL introduces a process in which a decision with a legal or similarly significant effect is made solely by automated processing, we will provide appropriate information about that processing and the safeguards and rights available to the individual, including the ability to obtain human intervention and challenge the decision where applicable.

We will assess AI-enabled processing before implementation, including through a Data Protection Impact Assessment where required, and will apply appropriate measures relating to data minimisation, security, accuracy, fairness, transparency and human oversight.

What Lawful Basis Does PCL Have for Using Information About Me?

Data Protection law requires that we only use your personal data if we have a lawful basis to do so. Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.

c) processing is necessary for compliance with a legal obligation to which the controller is subject.

d) processing is necessary to protect the vital interests of the data subject or of another natural person.

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.

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

Data protection law requires that we set out the legal basis for holding and using information about you. We have set out the various reasons we use information about you and alongside each, the legal basis for doing so.

For the purpose of delivering your direct health care and sharing your information we use Article 6(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.

Where we have to share your information because we are required to do so under law, we use Article 6(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.

Given that some information we hold about you is particularly sensitive (as described above), we need an additional legal basis which we have set out below explaining our reason for this.

For the purpose of delivering your direct health care and sharing your information we use Article 9(h) – health or social care.

Where and for How Long Does PCL Store Information about Me?

The majority of the information that we hold about you is held securely in the United Kingdom and stored electronically on secure servers and in paper format.

However, some information may be stored outside the European Economic Area (EEA).

We retain your records for certain periods (depending on the record) under our retention of records policy. PCL follows the recommended best practices contained in the NHS Records Management Code of Practice. This is to ensure that information is properly managed and is available whenever and wherever there is a justified need for that information, including:

To support patient care and continuity of care

To support evidence-based clinical practice

To assist clinical and other audits

To support our public task

To meet legal requirements

Your records may not be retained in hard copy form where a digital copy exists. If you would like more detailed information on this, please contact us (contact details above).

What Rights Do I Have?

Under certain circumstances, you have rights under data protection laws in relation to any personal information that we hold about you.

If you wish to exercise any of the rights set out below, please contact us using the contact details set out above. Details of your rights are set below:

The right to be informed

This privacy notice forms part of that, but we also aim to keep you fully informed during your consultations, via our communications to you and using posters in healthcare settings.

The right to access your personal information

You are usually entitled to a copy of the personal information we hold about you and details about how we use it.

Your information will usually be provided to you in the form you request, if we are unable to do that, we will inform you. If you have made the request electronically (e.g. by email) the information will be provided to you by electronic means where possible.

Under data protection law we must usually confirm whether we have personal information about you. If we do hold personal information about you, we usually need to explain to you:

The purposes for which we use your personal information.

The types of personal information we hold about you.

Who your personal information has been or will be shared with.

Where possible, the length of time we expect to hold your personal information. If that is not possible, the criteria we use to determine how long we hold your information for.

If the personal data we hold about you was not provided by you, where we obtained the information.

Your right to ask us to amend or delete your personal information (if appropriate).

Your right to ask us to restrict how your personal information is used or to object to our use of your personal information (if appropriate).

Your right to complain to the Information Commissioner's Office.

We also need to provide you with a copy of your personal information.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

We may need to request specific information from you to help us confirm your identity (which will be proportionate) and ensure your right to access your personal information (or to exercise any of your other rights). We may also contact you to ask you for further information in relation to your request to speed up our response.

We respond to all requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

The right to request correction of your personal information

We take reasonable steps to ensure that the personal information we hold about you is accurate, complete, and up to date. However, if you do not believe this is the case, you can ask us to update or amend it.

The right to request erasure of your personal information

In some circumstances, you have the right to request the erasure of the personal information that we hold about you. This is also known as the 'right to be forgotten.' However, there are exceptions to this right and in certain circumstances we can refuse to delete the information in question.

The right to restrict the processing of your personal information

In some circumstances, you have the right to object to the processing of your personal information. This would usually apply to processing for other purposes other than your direct healthcare (i.e., research).

The right to request a transfer of your personal information

In some circumstances, we must transfer personal information that you have provided to us to you or (if this is technically feasible) another individual/organisation of your choice. The information must be transferred in an electronic format.

The right to object

You can ask us to stop processing your information for any other purposes other than your healthcare.

The right not to be subject to automatic decisions and profiling

You have a right to not be subject to automatic decisions (i.e., decisions that are made about you by computer alone) that have a legal or other significant effect on you.

The right to withdraw your consent

You have the right to withdraw your consent where we rely upon this as a legal ground for processing your information.

To apply any of the Individual Rights above please contact the Data Protection Officer.

National Data Opt-Out

We review our data processing on an annual basis to assess if the national data opt-out applies. This is recorded in our Record of Processing Activities. All new processing is assessed to see if the national data opt-out applies. If any data processing falls within scope of the National Data Opt-Out we use MESH to check if any of our service users have opted out of their data being used for this purpose.

At this time, we do not share any data for planning or research purposes for which the national data opt-out would apply. We review all of the confidential patient information we process on an annual basis to see if this is used for research and planning purposes. If it is used, then individuals can decide to stop their information being shared for this

purpose. You can find out more information at https://www.nhs.uk/your-nhs-data-matters/.

The Right to Complain to the Information Commissioner's Office

You have the right to complain to us if you feel any of your rights under data protection have been breached or if have concerns about how we handle, use or secure your data. You can complain to us in the first instance: email / phone.

Phone: 0116 380 0590

Email: pcl.datagovernance@nhs.net

Data Protection Officer: Tania Palmariellodiviney — Tania@dataprivacysimplified.co.uk

If you are not satisfied with the outcome of your complaint, you have the right to complain to the Information Commissioner's Office.

Making a complaint will not affect any other legal rights or remedies that you have.

More information can be found on the Information Commissioner's Office website: https://ico.org.uk/ and the Information Commissioner's Office can be contacted by post, phone, or email as follows:

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

Tel: 0303 123 1113 (local rate) or 01625 545 745 (if you prefer to use a national rate number)

Fax: 01625 524 510

Email: casework@ico.org.uk

For further questions or to exercise any rights set out in this Privacy Notice, please contact us on the contact details provided above to request to speak to the Data Protection Officer.

Please note that this privacy notice applies to PCL and the information we collect about you only. For any services, other parties or websites mentioned in this privacy notice or on our website, we do not accept liability, and we advise you to read their privacy notices.

References

ICO. “Information Commissioner’s Office.” Ico.org.uk, ICO, 21 Mar. 2023, ico.org.uk/.

NHS. “Overview – Choose If Data from Your Health Records Is Shared for Research and Planning.” Nhs.uk, 23 May 2018, www.nhs.uk/your-nhs-data-matters/.

digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out