



ROTTON PARK MEDICAL CENTRE Privacy Notice for Patients

Data Protection Privacy Notice for Patients

Introduction:

This privacy notice lets you know what happens to any personal data that you give to us, or any information that we may collect from you or about you from other organisations.

This privacy notice applies to personal information processed by or on behalf of the practice.

This Notice explains

- Who we are and how we use your information
- Information about our Data Protection Officer
- What kinds of personal information about you we hold and what information we use (process)
- The legal grounds for processing your personal information (including when we share it with others)
- What to do if your personal information changes
- For how long your personal information is retained/stored by us
- What your rights are under Data Protection laws

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) became law on 25th May 2018. The GDPR is a single EU-wide regulation on the protection of confidential and sensitive (special) information, the DPA 2018 deals with elements of UK law that differ from the European Regulation, both came into force in the UK on the 25th May 2018, repealing the previous Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 the practice responsible for your personal data, and referred to at the Data Controller, is ROTTON PARK MEDICAL CENTRE.

This Notice describes how we collect, use, and process your personal data, and how in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.



How we use your information and the law

ROTTON PARK MEDICAL CENTRE will be what is known as the 'Data Controller' of your personal data.

We collect basic personal data about you and location-based information. This includes name, address and contact details such as email address and mobile number etc.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious beliefs, (if required in a healthcare setting) ethnicity, and sex life information that are linked to your healthcare; we may also receive this information about you from other health providers or third parties.

What are your rights over your personal data?

As an individual you have the following rights over your personal data that we hold:

Right to be informed – you have the right to be informed on how we handle, process, and share your personal information; this privacy notice ensures we as a practice satisfy this right.

Right to access your personal information– you can request access to and/or copies of the personal data we hold about you, free of charge (subject to exemptions) and provided to you within one calendar month. We request that you provide us with adequate information to process your request, such as providing full name, address, date of birth, NHS number and details of your request and, where necessary, any documents to verify your identity so we can process the request efficiently. On processing a request there may be occasions when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you. However, if the other person mentioned in your records was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that information.

To request a copy or request access to information we hold about you and/or to request information to be corrected if it is inaccurate, please contact: inderjitmarok@nhs.net 264, ROTTON PARK ROAD, EDGBASTON, BIRMINGHAM, WEST MIDLANDS B16 0LU

Right to rectification - The correction of personal data when incorrect, out of date or incomplete will be acted upon within one calendar month of receipt of such a request. Please ensure ROTTON PARK MEDICAL CENTRE has the correct contact details for you at all times.

Right to erasure - Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose which it was originally collected or processed it for of if you wish to withdraw your consent after you have previously given your consent

Right to restrict processing – Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that you can limit the way that the practice uses your data. This is an alternative to requesting the erasure of your data.



Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction.

Right to data portability - The right to data portability gives individuals the right to receive personal data they have provided to the Practice in a structured, commonly used and machine-readable format (i.e email, upload to a portable device etc.).

Right to object to processing – you have the right to object to processing, however please note if we can demonstrate compelling legitimate grounds which outweighs your interest, then processing can continue. If we did not process any information about you and your health care it would be very difficult for us to care and treat you.

Rights in relation to automated decision making and profiling - Automated individual decision-making is a decision made by automated means (i.e a computer system) without any human involvement.

Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

NHS health records may be electronic, paper-based or a mixture of both. We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

Records about you may include the following information;

- Details about you, such as your address, your carer or legal representative and emergency contact details.
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments.
- Notes and reports about your health.
- Details about your treatment and care.
- Results of investigations such as laboratory tests, x-rays etc.
- Relevant information from other health professionals, relatives or those who care for you.
- Contact details (including email address, mobile telephone number and home telephone number)

To ensure you receive the best possible care, your records are used to facilitate the care you receive, including contacting you. Information held about you may be used to help protect the health of the public and to help us manage the NHS and the services we provide. Limited information may be used within the GP practice for clinical audit to monitor the quality of the service we provided.



How do we lawfully use your data?

We need your personal, sensitive, and confidential data in order to provide you with healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with:

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

Article 9 (2) (h) 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

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from this GP Practice. The identifying parts of your data are removed, analysis of your data is undertaken, and a risk score is then determined. This is then provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt-out of your data being used in this way in most circumstances; please see appendix A for further information and contact the practice if you wish to discuss opt-out preferences.

Individual Risk Management at a GP practice level however is deemed to be part of your individual healthcare and is covered by our legal powers above.

Our data processor for Risk Stratification is:

Medicines Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments. The reviews are carried out by the Clinical Commissioning Group's Medicines Management Team under a Data Processing contract with the Practice.

Patient Communication

The Practice would like to use your name, contact details and email address to inform you of NHS services, or provide information about your health/information to manage your healthcare or information about the management of the NHS service. There may be occasions where authorised research facilities would like you to take part in research in regard to your particular health issues, to try



improve your health., Your contact details may be used to invite you to receive further information about such research opportunities.

Safeguarding

The Practice is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently, and conscientiously applied with the wellbeing of all, at the heart of what we do.

Our legal basis for processing For the General Data Protection Regulation (GDPR) purposes is:

Article 6(1)(e) ‘...exercise of official authority...’.

For the processing of special categories data, the basis is:

Article 9(2)(b) – ‘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...’

Categories of personal data

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is possible that is necessary to obtain in order to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Sources of the data

The Practice will either receive or collect information when someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

Recipients of personal data

The information is used by the Practice when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e. their GP or mental health team).

Research

Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here:

<https://cprd.com/transparency-information>

The legal bases for processing this information

CPRD do not hold or process personal data on patients; however, NHS Digital (formally the Health and Social Care Centre) may process ‘personal data’ for us as an accredited ‘safe haven’ or ‘trusted



third-party' within the NHS when linking GP data with data from other sources. The legal bases for processing this data are:

- Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) - public interest in the area of public health
- Medical research and statistics: Article 6(e) and Article 9(2)(j) - public interest and scientific research purposes

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties include:

- Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.
- Delivery services (for example if we were to arrange for delivery of any medicines to you).
- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third-party processors can be supplied on request to the Data Protection Officer as below.

How do we maintain the confidentiality of your records?

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The General Data Protection Regulations 2016
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep information



about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and/or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Our practice policy is to respect the privacy of our patients, their families, and our staff and to maintain compliance with the General Data Protection Regulation (GDPR) and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for ROTTON PARK MEDICAL CENTRE an appropriate contract will be established for the processing of your information.

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the inderjitmarok@nhs.net in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details, and email address to inform you of other services that may benefit you. We will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt into such programmes if you are happy to do so.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.

This information is not shared with third parties or used for any marketing and you can unsubscribe at any time via phone, email or by informing the practice DPO as below.



Where do we store your information electronically?

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

No third parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place such as a Data Processing agreement. We have a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data.

[Please select and use which system paragraph relates to your Practice, delete ones which are not appropriate]

EMIS Web

The Practice uses a clinical system provided by a Data Processor called EMIS. Since June 2019, EMIS commenced storing your practice's EMIS Web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services ("AWS").

The data will remain in the UK at all times and will be fully encrypted both in transit and at rest. In doing this there will be no change to the control of access to your data and the hosted service provider will not have any access to the decryption keys. AWS is one of the world's largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the very highest levels of security and support.

TPP SystemOne

The Practice uses a clinical system provided by a Data Processor called TPP SystemOne.

The system is a secure centralised system which supports modules for every healthcare setting from primary care to hospitals, social care, and mental health. SystemOne provides clinicians and health professionals with a single shared Electronic Health Record (EHR) available in real time at the point of care.

The data will remain in the UK at all times and allows patient data to be shared securely across services—promoting efficiency and standardisation. Most importantly it enables services to improve the patient experience and deliver safer patient care.

InPS Vision

The Practice uses a clinical system provided by a Data Processor called InPS Vision.

The system is a secure system which enables collaborative working and shared care records between NHS and other health and social care organisations.



Vision is hosted in a secure data centre to NHS Connecting for Health GPsoc Level 4 standards with robust Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptographic protocols to provide secure communications. The system supports single sign on and role-based access.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations:

- NHS Trusts/Foundation Trusts
- GP's
- Primary Care Networks
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Private Sector Providers
- Other 'data processors' which you will be informed of

Any organisations which you routinely share data with should be listed above

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

Computer System of Choice

This practice operates a Clinical Computer System of Choice on which NHS Staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history, including allergies and medication.

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisations (as listed above). Wherever possible, their staff will ask for your consent before your information is viewed.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems. You can opt-out of this sharing of your records with our partners at any time if this sharing is based



on your consent.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for ROTTON PARK MEDICAL CENTRE an appropriate contract will be established for the processing of your information.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- where there is a serious risk of harm or abuse to you or other people.
- Safeguarding matters and investigations
- where a serious crime, such as assault, is being investigated or where it could be prevented.
- notification of new births
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS)
- where a formal court order has been issued
- where there is a legal requirement, for example if you had committed a Road Traffic Offence.

How long will we store your information?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at

<https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>

Destruction

This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal, we have the following responsibilities:

- to ensure that information held in manual form is destroyed using a cross-cut shredder or contracted to a reputable confidential waste company [name of shredding company used, if applicable] that complies with European Standard EN15713 and obtain certificates of destruction.
- to ensure that electronic storage media used to store, or process information are destroyed or overwritten to national standards.



Primary Care Networks

The objective of Primary Care Networks (PCNs) is for group practices working together to create more collaborative workforces which ease the pressure of GP's, leaving them better able to focus on patient care. The aim is for all areas within England to be covered by a PCN.

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

All GP practices are expected to come together in geographical networks covering populations of approximately 30–50,000 patients and take advantage of additional funding attached to the GP contract.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Access to your personal information

Data Subject Access Requests (DSAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

- Your request should be made to the Practice. (For information from a hospital or other Trust/ NHS organisation you should write direct to them.
- There is no charge to have a copy of the information held about you
- We are required to provide you with information within one month
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located information we hold about you at any time.

What should you do if your personal information changes?

You should tell us so that we can update our records please contact the Practice Manager as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

Objections/Complaints

Should you have any concerns about how your information is managed at the GP, please contact the inderjitmarok@nhs.net. If you are still unhappy following a review by the GP practice, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK Supervisory Authority as below.

Information Commissioner:
Wycliffe House
Water Lane



Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745

<https://ico.org.uk/>

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact the Practice Data Protection Officer, Caldicott Guardian or IG Lead.

If you would like to know more about your rights in respect of the personal data that we hold about you, please use the contact details below:

IG Lead:

inderjitmarok@nhs.net

Caldicott Guardian:

inderjitmarok@nhs.net

Data Protection Officer:

Hayley Gidman

Useful Links

Please find below some links to external webpages which you may wish to access to find out additional information:

- [Information Commissioners Office](#)
- [Information Governance Alliance](#)
- [NHS Constitution](#)
- [NHS Digital Guide to Confidentiality in Health and Social Care](#)
- [Health Research Authority](#)
- [Health Research Authority Confidentiality Advisory Group \(CAG\)](#)
- [National Data Opt Out](#)



Appendix A: National Data Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning.

Who can use your confidential patient information for research and planning?

It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

Making your data opt-out choice

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Will choosing this opt-out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt out securely online or through a telephone service. You can change your choice at any time. To find out more or to make your choice visit <https://www.nhs.uk/your-nhs-data-matters/> or call 0300 303 5678.

Please discuss with the IG Lead or Practice Manager for further details.