Privacy Notice

Patient Information

Introduction

West Derby Medical Centre is committed to being transparent about how it handles your personal information, to protecting the privacy and security of your personal information and to meeting its data protection obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The purpose of this Privacy Notice is to make you aware of how and why we will collect and use your personal information.

Who Are We?

We accept patients from the West Derby Area of Liverpool and currently have a list size of 12,500 patients. We offer Primary Care services between our core hours and extended hours on a Tuesday evening until 8:00pm

The Practice has a statutory responsibility and public duty to provide health care services, as instructed and guided by the Department of Health and Social Care (a ministerial department of Government within the United Kingdom).

The Practice can be contacted at:

Address: WDMC, 3 Winterburn Crescent, Liverpool L12 8TQ
Tel: 0151 317 6310
Email: WestDerby.mc@nhs.net

The Practice is a Data Controller and, as such, is registered with the Information Commissioner's Office. Its registration number is Z5053610

The Practice's Data Protection Officer (DPO) is:

Head of Information Governance
NHS Informatics Merseyside
Information Governance Team
Hollins Park
Winwick
Warrington
WA2 8WA
DPO.IM@imerseyside.nhs.uk

Why does the Practice need your Information?

West Derby Medical Centre keeps records about your health and treatment to ensure the care you receive is effective, of good quality and meets your needs. The Practice needs information about you to create a care record that enables its staff to identify and contact you easily and to ensure appropriate services are offered to you. Information about you is used to help deliver care services to you, which includes sharing with external organisations, where appropriate, so that the care services are integrated.

Information will also be used to contribute to the management of the Practice, which means your information will be used to ensure the Practice is paid for the services it provides or is held accountable for the quality of its services.

Whilst the Practice receives information from you when you come into contact with it, it also receives information about you from other individuals or organisations, such as hospitals or community services, when you receive treatment from them. The Practice needs enough information to be able to provide you with appropriate healthcare services.

Looking after your Information

West Derby Medical Centre has put in place measures to protect the security of your personal information. It has internal policies, procedures and controls in place to prevent your personal information from being accidentally lost or destroyed, altered, disclosed or used or accessed in an unauthorised way. In addition, we limit access to your personal information to those employees, other workers, contractors and other third parties who have a business need to know in order to perform their duties and responsibilities. Everyone working for the NHS has a contractual and legal duty to protect your information.

Personal information is held in accordance with the requirements of current Data Protection legislation. Anyone who receives information from us is also under a legal duty to keep it confidential and secure in accordance with Data Protection legislation.

West Derby Medical Centre also have in place procedures to deal with a suspected data security breach, and we will notify the Information Commissioner's Office (or any other applicable supervisory authority or regulator) and you of a suspected breach where we are legally required to do so.

What types of personal information do we collect about you?

There are two types of data that West Derby Medical Centre uses; personal and special category. Personal data means any information relating to a person who can be directly (e.g. by name or picture) or indirectly (e.g. by age, gender and post code) recognised. Special category data means:

- data concerning physical or mental health. (for example, details about your appointments or diagnosis)
- data revealing racial or ethnic origin.
- data concerning a person's sex life.
- data concerning a person's sexual orientation.
- genetic data. (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- data revealing religious or philosophical beliefs.
- data relating to criminal or suspected criminal offences.

The Practice keeps data on you relating to who you are, where you live, what you do, your family, your emergency contacts, possibly your friends, your employers, your habits, organisations involved in your care, your symptoms, problems and diagnoses, the reasons you seek help, your appointments, where, when and by whom you are seen, referrals to other health and social care providers, tests carried out both by the Practice and in other places, investigations and scans, treatments and outcomes of treatments, your medical treatment history, the observations and opinions of other healthcare workers, within and outside the NHS, as well as comments and reminders reasonably made by health and social care professionals in the Practice who are appropriately involved in your health care.

The Practice will maintain a record of your care that consists of things such as:

- any contacts you have with staff (e.g. visits and appointments),
- notes or a summary of discussions,
- treatment/care plans and results of any tests,
- results of investigations such as laboratory tests, x-rays, etc,
- relevant information provided from other professionals, relatives or those who know or care for you, and
- information on medicines, side effects and allergies.

Your information will primarily be held electronically. When registering for NHS care, all patients who receive NHS care are registered on a national database. This database is held by NHS England, a national organisation which has legal responsibilities to collect NHS data. Some of the Practice's databases also connect to this national database to ensure your details remain up-to-date. This means if you change your address with the Practice, the new address will be automatically uploaded to the national database and will be available to other health and social care providers involved in your care. The Practice also uses other databases that it is responsible for, either directly or through legal contracts with suppliers.

What is the purpose of processing data?

West Derby Medical Centre processes your data in order to:

- provide the appropriate services to you,
- review its standards of care to ensure they are safe and effective,
- teach or train healthcare professionals,

- review your suitability for and/or carry out audits and research,
- undertake service evaluation,
- participate in national health screening programmes to ensure only those who should be called for screening are called and those at highest risk are prioritised,
- ensure security and safety (e.g. for the prevention and detection of fraud and other serious crimes, assisting in the prevention and control of diseases, or recording images on CCTV cameras),
- manage complaints, concerns, legal claims and incidents, and/or
- make sure the Practice is paid for the services that it provides.

Lawful Basis for Processing

Under the National Health Service Act 2006 and the Health and Social Care Act 2012, West Derby Medical Centre is required by law to process your personal data in order to provide you with direct care. Therefore, under current Data Protection legislation (the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR) the processing of your **personal data** is necessary under:

- **UK GDPR 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."*

Where we process **special categories** of sensitive information relating to your physical and/or mental health, racial or ethnic origin, etc, we do so under:

- **UK GDPR 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 and services…."*

The Practice has an obligation to protect the health of the general public and where this is done your **personal data** will be processed under:

- **UK GDPR 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."*

Where we process **special categories** of sensitive information relating to protecting the health of the general public, we do so under:

- **UK GDPR Article 9(2)(i)** "*processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Domestic Law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."*

As a healthcare provider there are occasions where we need to process **personal and/or special category data** because someone is at risk of serious harm (e.g. life or death situations in emergencies or major incidents) and, where we do this, we will process the information under:

- **UK GDPR Article 6(1)(d)** *"processing is necessary in order to protect the vital interests of the data subject or of another natural person."*

  and

- **UK GDPR Article 9(2)(c)** *"processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent."*

Sometimes there are occasions when we are obliged to process information to comply with a court order, coroner's instruction, to prevent or detect crime or to comply with the law (e.g. to provide the Secretary of State with information and reports on the status, activity, and performance of the Practice). If we must do this with your information, we will ensure there is a legal justification for such processing, for example under:

- **UK GDPR Article 6(1)(c)** *"processing is necessary for compliance with a legal obligation to which the controller is subject."*

If we process your information for other purposes that are not described above, then we will seek your consent to do so before we process it.

Sharing Your Information

West Derby Medical Centre shares information with a range of organisations or individuals for a variety of lawful purposes, this may include:

- other healthcare professionals (e.g. hospitals, community services, ambulance services, etc),
- partner organisations who contribute to your long-term care (e.g. Primary Care Networks, NHS organisations, Integrated Care Systems, social services/local authorities, education, etc),
- Private, Voluntary Sector and/or Charity Providers who contribute to your care,
- parents, carers or guardians with parental responsibilities or legal responsibilities,
- NHS managers and the Department of Health & Social Care/NHS England for the purposes of planning, commissioning, managing, and auditing healthcare services.
- organisations we contract with to provide services to or on behalf of the Practice,
- community pharmacists who will provide patients with their medication following discharge from hospital,

- bodies with statutory investigative powers (e.g. NHS Resolution, the Care Quality Commission, General Medical Council, Nursing and Midwifery Council, Audit Commission or the Parliamentary and Health Service Ombudsman),
- Government departments for national screening programmes and other national initiatives (e.g. NHS England, UK Health Security Agency, or the Home Office), and
- Police and other emergency services, out-of-hours services, courts (including coroner's court), solicitors and tribunals and national inquiries.

Patient information will only be shared if it is for the provision of your care or required for our statutory function and legal obligations.

The Practice is involved in integrated care programmes working with other NHS, Local Authority, private, voluntary and charity organisations. Information about you may be shared with partners in these programmes where it is legal to do so and for the purposes of direct care.

Any disclosures will be considered on a case-by-case basis to determine if they are appropriate and what the legal basis is for sharing. If the sharing goes ahead, only the minimum personal data necessary for the specific purposes and circumstances will be shared, with all suitable security controls in place. Any organisations receiving person-identifiable information from us are legally obligated to protect it.

The Practice will not share your information for marketing, social media, or insurance purposes unless it has your consent to do so. If you do consent to this, you have the right to withdraw your consent to the processing at any time.

Information provided under the Freedom of Information Act 2000 will not include person-identifiable details about patients.

GP Connect Service

GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patients care, leading to improvements in both care and outcomes. GP Connect is not used for any purpose other than direct care.

Authorised Clinicians such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS England (previously NHS Digital) service called GP connect.

The NHS 111 service & IGPC PCN will be able to book appointments for patients at GP practices and other local services.

National Care Records Services

National Care Records Service (NCRS) replaced Summary Care Record (SCR) during 2023, NCRS is a service that allows health and social care professionals to access

and update a range of patient and safeguarding information across regional Integrated Care Services (ICS) boundaries.

NCRS enables healthcare professionals, in any health or care setting, to access a summary of health and care information to support that patient's direct care.

Primary Care Networks

The objective of Primary Care Networks (PCNs) is to group practices together to create more collaborative workforces that ease the pressure on GPs, leaving them better able to focus on patient care. All areas within England are covered by a PCN.

PCNs form a key building block of the NHS Long Term Plan. Bringing 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 integrate with the wider health and care system more easily.

PCNs have been formed in geographical networks. The Practice is part of iGPC PCN This means that the PCN may share your information with other practices within Igpc PCN to provide you with your care and treatment.

Risk Stratification

Risk stratification is a mechanism used to identify and manage those patients deemed as being at high risk of requiring urgent or emergency care. Usually this includes patients with long-term conditions, e.g. cancer, chronic obstructive pulmonary disease (COPD), diabetes, etc. Your information is collected from several sources, including the Practice. This information is shared with NHS Cheshire and Merseyside who process it on our behalf. A risk score is given to patients which is shared with your GP so they can decide on any necessary actions to ensure that you receive the most appropriate care.

For further information, please see NHS Cheshire and Merseyside's Privacy Notice, which is available at https://www.cheshireandmerseyside.nhs.uk/about/how-we-work/privacy-notice/.

Invoice Validation

Invoice validation is an important process in ensuring that your care is paid for correctly. It involves using your NHS number to check that the Integrated Care Board (ICB) is responsible for paying for your treatment or if it has been funded through specialist commissioning, which NHS England will pay for. As such, West Derby Medical Centre may share your name, address, NHS number, and treatment date with NHS Cheshire and Merseyside Integrated Care Board under:

- **UK GDPR Article 6(1)(c**) *"the processing is necessary for compliance with any legal obligation to which the controller is subject.*"

For further information, please see NHS Cheshire and Merseyside's Privacy Notice, which is available at https://www.cheshireandmerseyside.nhs.uk/about/how-we-work/privacy-notice/.

Safeguarding

Some members of society are recognised as needing protection, for example children and vulnerable adults. If a person is identified as being at risk from harm, West Derby Medical Centre staff are expected as professionals to do what they can to protect them. In addition, they are bound by specific laws that exist to protect individuals. This is called "Safeguarding."

Where there is a suspected or actual safeguarding issue the Practice will share relevant information that it holds with other relevant agencies, regardless of whether or not the individual or their representative agrees. The laws that allow this processing to be undertaken without consent are the Children Act 1989 (Section 47) and the Care Act 2014 (Section 45).

Research

Research in the NHS is essential in helping to improve the health and wellbeing of the population and is included within the NHS Constitution. There is also evidence to suggest that when healthcare organisations engage in research, it is likely to have a positive impact on their performance and patient outcomes. As such, West Derby Medical Centre is proud to be a research active organisation, and it is dedicated to supporting clinical research. Its staff view care records in order to offer new research opportunities to patients and carers, to support the development of treatments and improve the way the Practice delivers healthcare.

The Practice only participates in research where there is an agreed, clearly defined reason for the research and that it is likely to benefit healthcare and patients. Such proposals will normally have a consent process, ethics committee approval and will be in line with the principles of Article 89(1) of UK GDPR.

Identifiable data will be ***shared*** with researchers either under:

- **UK GDPR Article 6(1)(c)** "*the data subject has given explicit consent to the processing of his or her personal data for one or more specific purposes.*"

  and

- **UK GDPR Article 9(2)(a)** "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes….*"

In the above instance, the common law duty of confidentiality is met by explicit consent, however, where the law allows, without consent, this is permissible under:

- **UK GDPR 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."*

  and

- **UK GDPR 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 and services…."*

  and

- **UK GDPR Article 9(2)(j)** *"processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes…"*

In the above instance, the common law duty of confidentiality is set aside by Section 251 support.

For further information, please go to https://www.hra.nhs.uk/information-about-patients/.

Your Rights

Data Protection laws give you rights in respect of the personal information that we hold about you. These are:

1. **To be informed why, where and how we use your information.**

2. **To ask for access to your information.**
   You have a legal right to access the personal information held about you by the Practice. You can obtain this information at any time by making a Subject Access Request. The Practice has one calendar month to provide the information to you. However, you do not have the right to access information that:

   - has been provided in confidence by someone else without consenting for you to see it,
   - relates to serious criminal offences, and/or
   - could cause physical or mental harm to you or someone else.

   Parents/carers/legal guardians can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

   Anyone requesting access to records will be asked to provide copies of identification documents to verify the lawfulness of their request.

To request access to records the Practice holds, please contact the Practice by emailing WestDerby.MC@nhs.net.

Another way to access your records is through the NHS App (or other approved patient-facing services apps). For further information on this, please go to https://transform.england.nhs.uk/information-governance/guidance/access-to-patient-records-through-the-nhs-app/.

3. **To ask for your information to be corrected if it is inaccurate or incomplete.**
   You have the right to have any inaccuracies in the data we hold about you corrected. However, if the data we hold is accurate, but you disagree with it, you should note that there is no right to have accurate medical records deleted except when ordered by a court of law. For further information about correcting inaccuracies, please see the guidance on Requesting Amendments to Health and Social Care Records (see link below) or contact the Practice by emailing WestDerby.MC@nhs.net

   https://transform.england.nhs.uk/information-governance/guidance/amending-patient-and-service-user-records/

4. **To ask for your information to be deleted or removed where there is no need for us to continue processing it.**
   You have the right to ask for your information to be removed, but if we require this information to provide you with appropriate medical services and diagnoses for your healthcare, then removal may not be possible. Please contact the Practice to discuss this further.

5. **To ask us to restrict the use of your information.**

6. **To ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information.**
   You have the right to request your information be transferred to another organisation. Please contact the Practice to discuss further.

7. **To object to how your information is used.**
   People who have access to your information will only have access to that which they need to fulfil their roles. You have the right to object to the Practice sharing your data in these circumstances, but the Practice has an overriding responsibility to do what is in your best interests and could still share the information even if you have objected. This will only be done with a valid legal justification.

   You have the right to object to some or all of your information being processed. However, please note that this is a right to raise an objection, which is different from having an absolute right to have your wishes granted in every circumstance. In certain circumstances the Practice will need to continue to process your information in order to provide you with the care you need

8. **To challenge any decisions made without human intervention (automated decision making)**

General Practice Extraction Service

General Practice Extraction Service (GPES) is a centrally managed, primary care, data extraction service that is in place across England, and is managed by NHS England.

GPES can collect 2 different types of information:

- effectively anonymised data that does not reveal an individual's identity.
- Patient-identifiable data (PID), that may identify an individual, such as a name, date of birth or postcode.

PID data is only used when information is permitted by law or supports direct benefits to patient care.

The purpose of GPES is to extract and compare data from across the NHS, allowing data to be turned into accurate and usable management information; this in turn leads to improvements in patient care and greater efficiency across the service as a whole.

For further information please access this link

National Data Opt-Out

National data opt-out was introduced in England in May 2018, following recommendations from the National Data Guardian. The service allows individuals to choose to opt out of having their confidential patient information shared for reasons beyond their individual care, for example for research and planning.

This means patients have more control over how their information is used and gives them the opportunity to make informed choices about whether they wish their confidential patient information to be used just for their individual care and treatment or also used for research and planning purposes. For further information, and/or to opt out, please visit https://www.nhs.uk/your-nhs-data-matters/. You can change your mind about your choice at any time.

You can also opt-out of some of the national screening programmes. For further information, please go to https://www.gov.uk/government/publications/opting-out-of-the-nhs-population-screening-programmes.

West Derby MC is currently compliant with the national data opt out policy and applies the policy to its data when necessary.

How long do we retain your records?

All our records are retained and destroyed in line with the NHS Records Management Code of Practice which set out the appropriate length of time each NHS record is held for. We do not keep your records for longer than necessary.

All records are destroyed confidentially once their retention period has been met and West Derby Medical Centre has made the decision that the records are no longer required.

Communicating with you

By providing West Derby MC with your contact details, we will communicate with you about your healthcare. This may be via a variety of ways e.g.

- Telephone (landline or mobile number)
- Text Messge (mobile number)
- Secure Email
- Approved Patient Portals / Apps e.g. NHS App

You can inform the practice of your preferred communication method and choose to opt out the ways you do not wish to be contact by e.g. text message. Any opt outs will be noted on your records, so Practice staff know how you wish to be contacted. You can change your mind at any time by informing the Practice.

You are responsible for ensuring you provide the Practice with correct contact details. You must inform the Practice of any changes. This will ensure you don't miss any information.

Telephone System

West Derby MC telephone system records all telephone calls. Recordings are retained for up to three years and are used periodically for the purposes of seeking clarification where there is a dispute as to what was said and for staff training. Access to these recordings is restricted to named senior staff.

Closed Circuit TV

West Derby MC has installed and uses Closed Circuit TV (CCTV) within its premises to help reduce the fear of crime for patients, staff, and visitors to our site(s) and to protect our premises and assets from criminal activity. In addition, CCTV may be used to monitor difficult to observe areas where patient or public safety could be compromised. If an incident occurs, the CCTV footage may be shared with the police for the purposes of investigating a crime. The Practice ensures that the use of CCTV complies with all relevant regulatory acts of law. The Practice Director is the data controller for the CCTV installed and used at the Practice.

Transferring Outside of the UK

West Derby MC does not routinely transfer information outside of the UK, but if there is a need to do so it will be done in a way that ensures the security of the information is to an equivalent standard as that used internally by the Practice when processing your information.

Practice Website

You can browse the Practice's website without disclosing personal data. The Practice uses cookies for its website. These are small text files that contain information about you, which are stored automatically on your computer by the website. Cookies are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org.

The Practice also uses Google Analytics[1] to collect information about how visitors use its website. The information is used to compile reports and to help improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website, where visitors have come to the website from and the pages they visited. To opt out of being tracked by Google Analytics across all websites, visit http://tools.google.com/dlpage/gaoptout.

The Practice's website contains links to other (external) sites. The Practice is not responsible for the privacy practices and content of these sites. The Practice encourages you to be aware of this when you leave its site and to read the privacy statements on the other websites.

Use of Third-Party Companies

When we use a third-party service provider to process data on our behalf, 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. An example of functions that may be carried out by third parties includes:

- 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); systems which facilitate appointment bookings or electronic prescription services; document management services etc.

Automated Decision Making

[1] https://policies.google.com/privacy/update

West Derby MC uses AI for automated decision making when signposting patients as part of its use of Paco Blinx software. The Practice does not carry out any automated decision making where AI solely decides on what care or treatment a person should receive. A health and care professionals will always make the final decision. The Practice may also use instances of AI that use automated decision making to improve efficiency, which do not use personal data.

Changes to this Privacy Notice

West Derby MC reserve the right to update or amend this Privacy Notice at any time, including where West Derby MC intend to further process your personal information for a purpose other than that for which the personal information was collected or where we intend to process new types of personal information. We will update this Privacy Notice when we make significant updates or amendments. We may also notify you about the processing of your personal information in other ways.

This Privacy Notice was last updated 30TH March 2026

Right to Complain

The Practice aims to make sure that the services it delivers are provided to the highest standard. If you have any concerns about the way the Practice has handled its data, you can raise your concerns or make a complaint by emailing WestDerby.MC@nhs.net.

Alternatively, you can complain to the Information Commissioner's Office by emailing casework@ico.org.uk or phoning 0303 123 1113.