# PARK VIEW SURGERY

## Patient Privacy Notice

*How we use your information to provide healthcare and run our services*

www.parkviewsurgerynhs.co.uk

| Item | Details |
|---|---|
| Document type | Patient-facing privacy notice |
| Practice / Data Controller | Park View Surgery |
| Practice privacy contact | Liz Butler, Practice Manager, Park View Surgery<br>pvs.parkviewadmin@nhs.net |
| Data Protection Officer | Dr Jon Rylance<br>pvs.parkviewadmin@nhs.net |
| Caldicott Guardian / IG Lead | Dr Julia Smith<br>pvs.parkviewadmin@nhs.net |
| Date reviewed | May 2026 |
| Next review due | May 2027, or sooner if legislation, NHS guidance, systems, suppliers or data-sharing arrangements change |

This notice explains what personal information we collect, why we collect it, how we use it, who we may share it with, how long we keep it, and your rights. It should be read alongside the Practice Privacy Policy, Information Governance Policy, Subject Access Request procedure and Complaints procedure.

### Contents

## 1. Summary - how we use your information

Park View Surgery keeps medical records so that we can provide safe, effective and joined-up care. We are legally required to protect your confidentiality and to comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the common law duty of confidentiality and relevant NHS requirements.

We use information to:

- provide diagnosis, treatment, prescriptions, referrals, test results and follow-up care;
- support appointments, registration, NHS App and online services, text messages, letters and other communications;
- work with other health and social care professionals involved in your care;
- check and improve the quality and safety of our services, including audit and clinical governance;
- meet legal, regulatory, NHS contractual, safeguarding and public health requirements;
- respond to complaints, incidents, subject access requests and information rights requests;
- support approved research, planning and service evaluation where this is lawful, transparent and appropriately safeguarded.

We only use the information we need for the relevant purpose. Access to confidential patient information is limited to people who need it for their role and who are bound by confidentiality obligations.

## 2. Who we are and how to contact us

Park View Surgery is the Data Controller for the personal information it holds about registered patients, former patients, carers, representatives, complainants and people who use or contact our services. In some situations, we may be a joint controller with other health or social care organisations, or a processor acting on another organisation's instructions.

Please contact the Practice Manager if you have questions about this notice, want to exercise your information rights, or have a concern about how your information has been used.

| Contact point | Details |
|---|---|
| Practice | Park View Surgery, Haverflatts Lane, Milnthorpe and<br>New Street Surgery, 21 New Street, Carnforth |
| Website | www.parkviewsurgerynhs.co.uk |
| Practice privacy contact | Liz Butler, Practice Manager, Park View Surgery<br>pvs.parkviewadmin@nhs.net |
| Data Protection Officer | Dr Jon Rylance<br>pvs.parkviewadmin@nhs.net |
| Caldicott Guardian / IG Lead | Dr Julia Smith<br>pvs.parkviewadmin@nhs.net |

## 3. What information we collect

We may collect and use the following information where it is relevant and necessary:

- identity and contact details, including name, date of birth, NHS number, address, telephone number, email address and communication preferences;
- registration information, previous GP details, next of kin, carers, representatives and nominated pharmacy;
- health records, consultation notes, diagnoses, symptoms, observations, care plans, medication, allergies, immunisations and safeguarding information;
- test results, pathology, imaging, screening information and reports from hospitals or other care providers;
- appointments, visits, telephone calls, correspondence, referrals, prescriptions, tasks and administrative notes;
- information submitted through online consultation systems, the NHS App, text messages, email, video or telephone services where these are used;
- information about complaints, feedback, incidents, claims, reports, insurance or medical report requests;
- information from other organisations involved in your care, such as hospitals, community services, social care, pharmacies, ambulance services, NHS 111 and out-of-hours providers.

We receive information from other organisations so that your GP record remains up to date. For example, hospitals send discharge summaries, outpatient letters and test results, and community teams may send updates about care they have provided.

## 4. Why we use your information

### 4.1 Direct care

Our main purpose is to provide direct health and care services to you. This includes assessment, diagnosis, treatment, prescriptions, referrals, care planning, follow-up, prevention, screening, medicines management and coordination with other professionals involved in your care.

### 4.2 Registration and NHS administration

When you register for NHS care, your basic demographic details are held on national NHS systems such as the Personal Demographics Service. This supports accurate identification, NHS number management, contact details, GP registration and safe linkage of records across care settings.

### 4.3 Quality, safety and service improvement

We use information to check and review the quality of care we provide. This includes clinical audit, significant event review, medicines safety, appointment management, workforce planning, training, supervision and service improvement. We use anonymised or de-identified information wherever possible.

### 4.4 Identifying patients who may need extra care

We may use computer searches or risk stratification tools to identify patients who may be at higher risk of certain conditions, complications or unplanned hospital admission. This helps us offer reviews, advice or extra support earlier. Any action about your care will be reviewed by appropriate clinicians; we do not make decisions about your care solely by automated means that have legal or similarly significant effects.

### 4.5 Safeguarding and protection from harm

We may share information where this is necessary to protect children, adults at risk, staff or members of the public from harm. We do not need your consent where sharing is required by law, necessary for safeguarding, or justified in the public interest.

### 4.6 Research, planning and population health

We may support approved research, planning, public health and service evaluation. Some projects ask patients for consent before taking part. Some use anonymised or pseudonymised information. Where confidential patient information is used for research or planning, this will only happen where there is a lawful basis, appropriate approvals and safeguards, and where the national data opt-out is applied unless an exemption applies.

## 5. How we share information for your care

We may share relevant information with other health and social care professionals who are directly involved in your care. This may include hospitals, community services, mental health services, pharmacies, ambulance services, social care, out-of-hours services, NHS 111 and urgent or emergency care providers.

### 5.1 Primary Care Network and local teams

Park View Surgery works with Ash Trees Surgery as part of Carnforth and Milnthorpe Primary Care Network. PCN staff and services may include roles such as pharmacists, social prescribers, first contact physiotherapists, paramedics, mental health practitioners and care coordinators. Where PCN staff are involved in your care, they may access relevant parts of your record on a need-to-know basis, subject to confidentiality, role-based access controls and local data sharing arrangements.

### 5.2 Medicines optimisation and prescribing support

Medicines optimisation staff, including pharmacists working for or with the Practice, PCN or local Integrated Care Board, may access relevant information to support safe prescribing, medication review, prescribing queries, monitoring and medicines safety. Access must be necessary, proportionate and subject to confidentiality and audit controls.

### 5.3 Shared care records, GP Connect, Summary Care Record and National Care Records Service

Your information may be available to authorised health and care staff through approved shared record systems for direct care. This may include local shared care record arrangements, GP Connect, the Summary Care Record and the National Care Records Service. These systems are intended to help professionals involved in your care see important information, such as medication, allergies, adverse reactions and other relevant clinical information, especially in urgent or emergency situations.

Only authorised staff should access these systems, and access should be limited to what is necessary for direct care. You can ask the Practice about your choices and any local shared care record arrangements.

## 6. Other ways we may use or share information

| Purpose | How information may be used or shared |
|---|---|
| Legal and regulatory duties | To meet NHS contractual requirements, CQC requirements, professional obligations, public health duties, court orders, coroner requests or other legal requirements. |
| Safeguarding | To share relevant information with safeguarding services, local authorities, police or other agencies where necessary to protect someone from harm. |
| Complaints, concerns and claims | To investigate and respond to complaints, incidents, concerns, claims or legal matters. Complaint records are not normally filed as part of the clinical record unless clinically relevant. |
| Research and planning | To support approved research, planning, commissioning and service evaluation, usually using anonymised or pseudonymised data. Confidential patient information will only be used where lawful and appropriately safeguarded. |
| Public health and communicable disease control | To support vaccination, screening, disease surveillance, infection control and public health functions where required or permitted by law. |
| Fraud prevention and security | To prevent or detect fraud, crime, misuse of NHS services, cyber incidents or security incidents where lawful and necessary. |
| Suppliers and processors | To use contracted suppliers such as clinical system providers, document management, SMS/email, online consultation, appointment, archiving, shredding, payroll or IT support providers. Contracts and safeguards must be in place. |

## 7. Partner organisations and service providers

Depending on the circumstances, we may share relevant information with:

- GP practices, PCN services, hospitals, NHS Trusts and Foundation Trusts;
- community services, mental health services, district nurses, specialist nurses, care homes and social care services;
- out-of-hours services, NHS 111, urgent care, ambulance services and emergency departments;
- pharmacies, dentists, opticians and other independent contractors involved in NHS care;
- Integrated Care Boards, NHS England, Primary Care Support England and other NHS bodies for statutory, contractual, registration, payment, assurance or service purposes;
- local authorities, education services, fire and rescue services, police, courts, coroners or safeguarding agencies where there is a lawful basis;
- voluntary and charitable organisations where they are involved in your care or support and sharing is lawful;
- auditors, regulators, professional advisers, insurers, legal representatives and complaints or investigation bodies where necessary;
- IT, communications, clinical system, document management, archiving, confidential waste and other suppliers acting under contract.
-

We do not sell your information. We do not share confidential patient information for marketing. Where information is shared, it must be lawful, necessary, proportionate and secure.

## 8. Patient choices, objections and opt-outs

### 8.1 Direct care sharing

You can ask questions or raise an objection about how information is shared for your direct care. We will consider your concerns carefully. In some circumstances, limiting sharing could affect the care you receive or create risks, and in some situations we may still need to share information because of a legal duty, safeguarding need or overriding public interest.

### 8.2 Type 1 opt-out

A Type 1 opt-out can be recorded by your GP practice to stop confidential patient information from your GP record being shared outside the Practice for purposes beyond your individual care, except where a legal exemption applies. Please speak to the Practice if you want to discuss or record a Type 1 opt-out.

### 8.3 National data opt-out

The national data opt-out lets you choose whether your confidential patient information can be used for research and planning. It does not affect your individual care. You can set, check or change your choice online or by using the NHS support routes listed in section 13.

### 8.4 Summary Care Record preferences

You can ask the Practice about your Summary Care Record and your preferences for additional information within it. Emergency and urgent care staff may rely on key information such as medicines, allergies and adverse reactions to provide safe care.

### 8.5 Limits to opt-outs

Opt-outs do not usually apply where information is used for your individual care, where there is a legal requirement, where information is needed for safeguarding or public health, where there is an overriding public interest, or where information has been anonymised so that you cannot be identified.

## 9. Your information rights

You have rights under data protection law. These rights may be limited in some circumstances, for example where a record contains information about another person, where disclosure could cause serious harm, where there is a legal restriction, or where information must be kept for clinical, legal or safeguarding reasons.

| Right | What this means |
|---|---|
| Right to be informed | You have the right to clear information about how your personal information is used. This notice is part of how we meet that duty. |
| Right of access | You can request a copy of information we hold about you. This is called a subject access request. You do not have to use a specific form, but forms can help us locate the information you need. |
| Right to rectification | You can ask us to correct factual inaccuracies. Clinical opinions cannot normally be changed just because you disagree with them, but you can ask for your view to be added. |
| Right to restriction | You can ask us to restrict processing in certain circumstances while concerns are considered. |
| Right to object | You can object to certain uses of your information. We will consider your objection, but may need to continue using information where there is a compelling lawful reason. |
| Right to erasure | This right is limited for health records because we usually have clinical, legal and NHS obligations to keep accurate records. |

| | |
|---|---|
| Right to data portability | This applies only in limited circumstances and is unlikely to apply to most GP record processing. |
| Automated decision-making | We do not make decisions about your care solely by automated means that have legal or similarly significant effects. Searches and risk tools support clinical review. |

Please contact the Practice Manager if you want to exercise any of these rights. Staff must pass requests to the Practice Manager promptly, even if the request is made verbally or informally.

## 10. Keeping information safe and confidential

All staff and authorised users must protect personal information and confidential patient information. We use appropriate technical and organisational measures to reduce the risk of unauthorised access, loss, misuse or disclosure.

- role-based access controls, smartcards or secure authentication and audit trails;
- confidentiality clauses, staff training and annual data security / information governance training;
- secure storage, clear desk arrangements, confidential waste and secure printing;
- approved secure methods for transferring information, remote access and mobile working;
- supplier due diligence, contracts and access controls for organisations that process information for us;
- incident reporting, breach assessment, lessons learned and Data Security and Protection Toolkit evidence;
- Data Protection Impact Assessments for high-risk processing or significant new systems or data uses.

Any actual or suspected data breach, confidentiality breach, near miss, loss of records, cyber incident or unauthorised access must be reported immediately. Where required, we will notify the Information Commissioner's Office within the statutory timescale and inform affected individuals where the legal threshold is met.

We do not routinely transfer your information outside the UK. Where a supplier or service involves international transfers, we will only use lawful transfer mechanisms and appropriate safeguards.

## 11. How long we keep records

GP medical records and related information are kept in line with the NHS Records Management Code of Practice and other legal, contractual, clinical and professional requirements. Retention periods are minimum periods and records may need to be kept longer where there is an ongoing care need, complaint, claim, safeguarding matter, audit, regulatory requirement, public inquiry or other legal reason.

Records that are no longer required will be disposed of securely using approved confidential waste, deletion, destruction or archiving processes. Staff must not delete, destroy or remove records outside approved procedures.

## 12. Complaints and concerns

Please contact the Practice Manager or Data Protection Officer if you are concerned about how your information has been used, shared or protected. We will handle data protection complaints promptly, fairly and in line with our complaints procedure and data protection requirements.

From 19 June 2026, data protection complaints requirements under the Data (Use and Access) Act 2025 require organisations to provide a clear complaints process, acknowledge complaints within 30 days where applicable, and respond without undue delay. The Practice will follow any statutory requirements and ICO guidance in force at the time.

If you remain dissatisfied, you can complain to the Information Commissioner's Office (ICO):

- Website: https://ico.org.uk/make-a-complaint/
- Telephone: 0303 123 1113
- Postal address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

### 13. Further information

You can find more information from the following sources:

- **National data opt-out / Your NHS Data Matters:** https://www.nhs.uk/your-nhs-data-matters/
- **Manage your national data opt-out choice:** https://your-data-matters.service.nhs.uk/
- **NHS England Digital - National Data Opt-Out:** https://digital.nhs.uk/services/national-data-opt-out
- **NHS England Digital - Summary Care Record:** https://digital.nhs.uk/services/summary-care-records-scr
- **NHS England Digital - GP Connect:** https://digital.nhs.uk/services/gp-connect
- **NHS England - Records Management Code of Practice:** https://transform.england.nhs.uk/information-governance/guidance/records-management-code/
- **Information Commissioner's Office:** https://ico.org.uk/

## Appendix A - UK GDPR transparency information

The following table summarises the information we are required to provide about common processing purposes. This table should be reviewed whenever services, systems, suppliers or sharing arrangements change.

| Requirement | Summary |
|---|---|
| Data Controller | Park View Surgery |
| Data Protection Officer | Dr Jon Rylance<br>pvs.parkviewadmin@nhs.net |
| Main purposes | Direct care, registration, appointments, prescriptions, referrals, shared care, safeguarding, quality and safety, complaints, legal compliance, audit, service improvement, research and planning where lawful. |
| Lawful basis - direct care | UK GDPR Article 6(1)(e) public task and Article 9(2)(h) health or social care. Common law confidentiality is met through direct care expectations or consent where required. |
| Lawful basis - legal duties | UK GDPR Article 6(1)(c) legal obligation and/or Article 6(1)(e) public task, with an Article 9 condition such as health or social care, public health, vital interests or substantial public interest depending on the purpose. |
| Lawful basis - safeguarding | UK GDPR Article 6(1)(c), 6(1)(d) or 6(1)(e), Article 9(2)(g), 9(2)(h) or 9(2)(i), and Data Protection Act 2018 Schedule 1 conditions where relevant. |
| Lawful basis - research/planning | Depends on the specific activity. May include Article 6(1)(e), Article 9(2)(j), approvals, safeguards, transparency and application of the national data opt-out where required. |
| Recipients | Health and social care providers, PCN services, ICB, NHS England, PCSE, public health bodies, regulators, safeguarding agencies, local authorities, emergency services, legal bodies, auditors, suppliers and processors where lawful and necessary. |
| Transfers outside the UK | Not routine. Where a transfer is required, appropriate safeguards and lawful transfer mechanisms will be used. |
| Retention | In line with the NHS Records Management Code of Practice and local retention procedures. |
| Rights | Be informed, access, rectification, restriction, objection, erasure where applicable, portability where applicable, and rights relating to automated decision-making. |
| Right to complain | Contact the Practice Manager or DPO first. You may also complain to the ICO if dissatisfied. |