RICHMOND SURGERY

Practice Privacy Notice

How we use your personal information

1. About this Privacy Notice

This privacy notice explains what information Richmond Surgery holds about you, why we use it, where it may come from, who we may share it with, how long it is kept and the rights you have in relation to your personal information.

Richmond Surgery is the Data Controller for the GP record that we create and maintain about you. We are responsible for ensuring that personal information is handled lawfully, fairly, transparently and securely.

2. Information We Hold About You

Your health record may be electronic, on paper or a mixture of both. We use appropriate working practices and technology to protect confidentiality and security.

- your name, address, date of birth, NHS number and contact details;
- details of carers, legal representatives and emergency contacts where relevant;
- appointments, consultations and other contacts with the Practice;
- notes and reports about your physical and mental health;
- details of treatment, medicines and care;
- results of investigations, including laboratory tests and imaging;
- information about referrals and care provided by other health and care organisations;
- information relevant to safeguarding and the safe provision of care; and
- telephone call recordings where calls are recorded by the Practice.

Telephone recordings are retained in accordance with the configured retention arrangements for the Practice telephone system. The Practice will confirm the precise current retention period before this notice is finalised.

3. Where We Obtain Information From

Most information is provided directly by you. We may also receive relevant information from other sources involved in your health and care, including hospitals, community services, pharmacies, other GP practices, NHS organisations, local authorities, screening and public health services, carers or relatives where appropriate, and other health and care professionals.

We only use information obtained from other sources where there is an appropriate legal and confidentiality basis for doing so.

4. Why We Use Your Information

We use personal information primarily to provide and coordinate your direct care. We may also use information where necessary for the management of NHS services, safeguarding, public health, medicines safety, clinical

audit, quality improvement, service planning, statutory reporting, commissioning, approved research and other purposes permitted or required by law.

Where information is used for planning, audit, statistics or service evaluation, identifiable information will not be used where anonymous or appropriately de-identified information is sufficient.

Research does not always rely on consent as its data protection or confidentiality basis. Where consent is required for a particular research activity, it will be sought. Other approved research may use a different lawful basis or statutory approval, and patients will be informed where required.

5. Third-Party Services and Information Sharing

To provide safe and effective services, Richmond Surgery shares information where necessary with other health and care organisations and uses carefully selected service providers. Appendix A gives further detail about significant data-sharing and processing activities.

Where an organisation processes personal data solely on our instructions, we will have appropriate contractual and data protection arrangements in place. Some organisations receiving information for their own statutory or care functions are separate Data Controllers rather than processors. The legal relationship depends on the particular service and data flow.

- IT, clinical system, document management and data-hosting providers;
- patient-facing communication, appointment and online consultation systems;
- electronic prescribing and pharmacy services;
- diagnostic, treatment and community health services;
- interpreting and translation services;
- remote monitoring and long-term condition support services;
- commissioning, public health and statutory NHS bodies; and
- other organisations that support the delivery, safety and governance of NHS care.

6. Extended Access and Care Provided by Other GP Services

Richmond Surgery participates in arrangements that enable patients to receive GP services outside normal Practice opening hours. Relevant information may be made available to authorised clinicians providing that direct care, subject to appropriate access controls and data-sharing arrangements.

The Practice currently identifies Hart Health Partnership and Crondall New Surgery as local practices involved in these arrangements. The commissioning/provider wording for this service will be confirmed against the current Hampshire and Isle of Wight arrangements before final approval.

7. Confidentiality and Security

We are committed to protecting your privacy and handling information in accordance with applicable law and NHS confidentiality and information governance requirements, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2026, where applicable;

- Human Rights Act 1998;
- Common Law Duty of Confidentiality;
- Health and Social Care Act 2012 and other relevant NHS legislation;
- Caldicott Principles; and
- NHS information security and records management requirements.

Staff and contractors with access to confidential information are required to protect it. Information may be shared without explicit consent where there is another lawful and appropriate basis, for example for direct care, safeguarding, statutory reporting, public health, prevention of serious harm, legal requirements or other permitted NHS functions. Only information that is necessary and relevant should be shared.

8. Data Controller and Data Protection Officer

Data Controller	Richmond Surgery Richmond Close Fleet Hampshire GU52 7US
Data Protection Officer	Taj Sallamuddin, leading the Data Protection Officer team Trusted Technology IG Services (TTIG) Email: TTIG@informationgovernanceservices.com Telephone: 0345 0348690 option 4

9. Lawful Basis for Processing

For the provision and management of health and care, Richmond Surgery will commonly rely on UK GDPR Article 6(1)(e) – processing necessary for a task carried out in the public interest or in the exercise of official authority – and Article 9(2)(h) – processing necessary for health or social care purposes.

Other lawful bases and statutory powers may apply to particular activities, including safeguarding, public health, legal obligations, approved research and national data collections. Appendix A describes the basis for significant processing activities where appropriate.

The Common Law Duty of Confidentiality is considered separately from the UK GDPR lawful basis. Consent may be relevant to confidentiality or participation in a particular service, but UK GDPR consent is not the routine lawful basis for processing information for direct care.

10. Your Rights

Your rights depend on the circumstances and lawful basis for the processing. They include, where applicable:

- the right to be informed about how your personal information is used;
- the right of access to your personal information (a Subject Access Request);
- the right to have inaccurate personal information corrected;
- the right to request restriction of processing in certain circumstances;
- the right to object to certain processing;
- the right to erasure in limited circumstances (this does not normally mean that an accurate clinical record can simply be deleted);

- the right to data portability where the legal conditions apply;
- the right to withdraw consent where processing is actually based on consent; and
- rights relating to solely automated decision-making and profiling where applicable.

A request may be made verbally or in writing. Some rights are not absolute and may be limited by law or by the basis on which information is processed. The Practice will explain the outcome if a request cannot be fully met.

11. Automated Decision-Making and Artificial Intelligence

Richmond Surgery uses digital systems, including Heidi Health for clinical documentation support. Clinicians remain responsible for reviewing and approving information entered into the clinical record.

The Practice does not intend to make solely automated decisions about patients that produce legal or similarly significant effects without meaningful human involvement. If such processing is introduced, this notice and any relevant Data Protection Impact Assessment will be updated.

12. International Transfers

Where a supplier or service involves access to or storage of personal data outside the United Kingdom, Richmond Surgery will ensure that an appropriate lawful transfer mechanism and safeguards are in place. Specific supplier arrangements are governed by contracts, data protection assessments and, where required, Data Protection Impact Assessments.

This section should be confirmed by the DPO against the Practice's current supplier register before final approval.

13. Retention of Records

Records are retained for the periods required by law and applicable NHS records-management guidance. Richmond Surgery follows the NHS Records Management Code of Practice 2021 and subsequent applicable national guidance.

Different categories of information have different retention periods. Information is securely disposed of when it is no longer required and there is no lawful reason to retain it.

14. National Data Opt-Out and Type 1 Opt-Out

Some uses of confidential patient information for purposes beyond individual care may be subject to the National Data Opt-Out. Patients can obtain current information about the National Data Opt-Out through NHS services.

Type 1 Opt-Out arrangements apply to certain extractions of confidential patient information from GP records for purposes other than individual care. Historic deadlines and COVID-era wording have been removed from this notice. Current national requirements will apply.

Opt-outs do not prevent information being used or shared where there is a legal requirement, an overriding public interest basis, or another applicable exemption.

15. Change of Details

Please tell the Practice if personal details such as your name, address, telephone number or other contact information change, or if information such as your date of birth is incorrect. Accurate and up-to-date information helps us provide safe care and communicate with you appropriately.

16. Complaints

If you have concerns about how Richmond Surgery uses your personal information, please contact the Practice or the Data Protection Officer in the first instance.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK's data protection regulator. Current contact information is available on the ICO website.

17. Review of this Notice

This notice will be reviewed regularly and updated when there is a significant change in how the Practice uses personal information, when services or suppliers change, or when legislation, ICO guidance or NHS requirements change. Where a new use of personal information requires patients to be informed, appropriate privacy information will be provided before or at the time the new processing begins.

Appendix A – Who We Share Information With and Why

Activity / Organisation	Purpose, legal basis and current status
Hampshire and Isle of Wight Integrated Care Board / NHS commissioning arrangements	Purpose: Planning, commissioning and management of local NHS services. Anonymous or aggregated information will be used where identifiable information is not required. Legal basis: Depends on the specific function and data flow, including statutory NHS functions and UK GDPR Articles 6 and 9 where personal data is required. Status: Replaces historic references to CCGs and the former Frimley transition wording. DPO / Practice confirmation required for any current identifiable data flows.
Individual Funding Requests / Commissioning Support	Purpose: To support consideration and funding of treatment that is not routinely commissioned where this applies to an individual patient. Legal basis: Determined by the current commissioning pathway and confidentiality arrangements. Recipient/service: Current HIOW ICB / commissioning support route to be confirmed. Historic NHS South, Central and West wording should not be assumed to remain accurate. DPO / Practice confirmation required.
Summary Care Record (SCR)	Purpose: To make key GP record information available securely to authorised health and care professionals for direct care, particularly urgent or unplanned care. Legal basis: Direct care; UK GDPR Article 6(1)(e) and Article 9(2)(h), together with applicable confidentiality arrangements. Note: Historic COVID-19 COPI wording has been removed. Current NHS arrangements and patient preferences apply.
CHASE – adult vaccination programmes	Purpose: To support shingles and pneumococcal vaccination activity and direct patient care. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h). Provider/role: Existing notice names Chase Search and Selection Limited. DPO / Practice confirmation required that the service and role remain current.
CHIE	Purpose: To provide authorised health and care professionals with relevant, up-to-date information from participating health and care organisations to support direct care. Legal basis: Direct care, commonly UK GDPR Article 6(1)(e) and Article 9(2)(h), with applicable confidentiality arrangements. Provider/role: Existing notice names NHS South, Central and West. DPO / Practice confirmation required for current controller/processor arrangements and current opt-out wording.
CHIA / population health analytics	Purpose: Population health analysis, service planning and research using de-identified or pseudonymised information where appropriate. Legal basis: Depends on the current data flow and commissioning arrangement. Provider/role: Existing notice names NHS South, Central and West. DPO / Practice confirmation required for current service name, role and opt-out position.
National GP data collections / GPES	Purpose: GP practices may be legally required to provide information for specified national collections, audits, planning, service improvement or other NHS functions. Legal basis: The applicable statutory direction or Data Provision Notice and

	relevant UK GDPR conditions for each collection. Examples retained from the previous notice include CVDPREVENT, physical health checks for people with severe mental illness and national obesity audit activity where current. Note: Historic COVID-19 pandemic extraction wording has been removed. DPO / Practice confirmation required for the current list of collections.
General Practice Data for Planning and Research / national secondary-use collections	Purpose: Where current national arrangements require or permit GP data to be used for health and care planning and research, information will be processed in accordance with the applicable national legal framework. Opt-outs: National Data Opt-Out and Type 1 Opt-Out arrangements apply where relevant. Note: The historic 23 June 2021 deadline and obsolete NHS Digital wording have been removed. Current NHS England arrangements apply.
Other GP practices / extended access	Purpose: To enable authorised clinicians in other GP practices to access relevant information when providing direct care to Richmond Surgery patients through shared or extended access services. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h), together with the Common Law Duty of Confidentiality and applicable direct-care sharing arrangements. Current local practices named by Richmond Surgery: Hart Health Partnership and Crondall New Surgery. Controller status: Receiving care providers may act as separate controllers for care they provide; DPO confirmation required for the specific shared-care arrangement.
Community nursing and community clinical services	Purpose: To support direct care provided by community teams, including services such as district nursing, diabetes, complex care, home visiting, leg ulcer, heart failure, multidisciplinary care and midwifery where applicable. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h), with applicable confidentiality arrangements. Current providers and controller relationships should be confirmed against HIOW arrangements.
Berkshire Primary Care – records digitisation	Purpose in existing notice: Collection, digitisation and final destruction of paper medical records under an NHS digitisation programme. Status: DPO / Practice confirmation required that this service is still active and that the provider and destruction arrangements remain current. Remove if no longer used.
Interpretation and Translation Services	Purpose: To provide spoken, non-spoken, telephone, video and document interpretation/translation where needed to support safe and accessible care. Legal basis: Direct care, commonly UK GDPR Article 6(1)(e) and Article 9(2)(h). Existing notice names Dals Translation and Interpretation Service and historic Frimley commissioning wording. Current HIOW provider and contractual role require confirmation.
TVS / Docobo – remote care and monitoring	Purpose: Remote care and monitoring through the DOC@HOME / relevant remote monitoring platform where currently commissioned. Legal basis: As specified by the applicable service and statutory arrangements. Status: DPO / Practice confirmation required that TVS, Docobo and the stated legal powers remain current.
Interface Clinical Services	Purpose: Existing notice describes use of anonymised data to support chronic disease management and identify patients who may benefit from preventative care. Legal basis and role: DPO / Practice confirmation required. If only anonymous

	information is processed, UK GDPR may not apply to that information; any identifiable processing must be separately described.
Lung Cancer Screening – InHealth	Purpose: To identify and invite eligible patients for lung health / lung cancer screening and support follow-up care. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h), subject to the current programme arrangements. Provider: InHealth, subject to Practice/DPO confirmation of the current local programme.
Medefer	Purpose: Existing notice states early diagnosis of prostate cancer. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h) where used for direct care. Status: DPO / Practice confirmation required that the service, purpose and controller/processor role remain current.
MedLink	Purpose: To support management of long-term conditions and routine care, including patient communication and collection of relevant health information. Legal basis: Direct care; UK GDPR Article 6(1)(e) and Article 9(2)(h). Role: Current processor/controller arrangements should be confirmed against the Practice contract and DPIA.
OMRON Hypertension Plus	Purpose: An invited digital service enabling patients to submit blood pressure and related information to support hypertension monitoring and preventative care. Legal basis: Direct care; UK GDPR Article 6(1)(e) and Article 9(2)(h), subject to the current service arrangements. Status: DPO / Practice confirmation required that this service remains in use.
OpenSAFELY / NHS England	Purpose: Secure analysis of pseudonymised GP data for approved research, clinical audit, service evaluation and health surveillance under national arrangements. Controller and legal basis: Governed by current NHS England directions and OpenSAFELY arrangements. Note: COVID-only wording has been removed because the service now supports broader approved purposes. DPO confirmation required for current transparency and opt-out wording.
Early Onset Type 2 Diabetes programme – Oviva	Purpose: To offer eligible patients a direct-care programme, with information shared as necessary for enrolment and delivery where the patient chooses to participate. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h) for health-care processing; patient choice/consent may also govern participation in the programme. Provider: Oviva UK Ltd, subject to confirmation that the programme remains current.
Heidi Health	Purpose: AI-assisted clinical documentation to support clinicians in creating consultation notes and reducing administrative burden. Clinicians review and approve the resulting clinical documentation. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h), with Data Protection Act 2018 Schedule 1 health and social care condition where applicable. Role: Heidi Health is identified by the Practice as a service provider/processor. Current contract, DPIA, data location and international-transfer safeguards should be confirmed by the DPO.
Healthy.io	Purpose: Home urine testing / kidney health monitoring for eligible patients, including contact and test-kit delivery where the programme is offered.

	Legal basis: Direct care, commonly UK GDPR Article 6(1)(e) and Article 9(2)(h). Status: Existing notice names Healthy.io. DPO / Practice confirmation required that the programme remains active and that current commissioning and retention wording is correct.
Community Children's Service – HCRG Care Group	Purpose: To provide community health services to children. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h). Provider: HCRG Care Group, subject to confirmation that this remains the current provider and that the data-sharing role is accurately described.
Anticoagulation database – LumiraDx	Purpose: To support anticoagulation monitoring and management for eligible patients. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h). Provider: Existing notice names LumiraDx. DPO / Practice confirmation required that the database/provider remains current.
Medicines optimisation / pharmacists	Purpose: To support safe, effective and cost-effective prescribing, medicines monitoring and medicines optimisation. Legal basis: Depends on whether the activity is direct care, statutory commissioning or anonymous service monitoring. Note: Historic references to Fareham & Gosport and South East Hampshire CCG have been removed. Current HIOW / PCN / provider arrangements require confirmation.
Judi's Wellbeing	Purpose in existing notice: Direct patient care to vulnerable patients using partner organisations. Legal basis: Existing notice cites Article 6(1)(e) and Article 9(2)(h). Status: DPO / Practice confirmation required that the service remains current and that the provider/controller details are accurate. Remove if no longer used.
Safeguarding / Multi-Agency Safeguarding arrangements	Purpose: To protect children and adults at risk and to enable appropriate safeguarding assessment, referral and multi-agency working. Legal basis: Statutory safeguarding duties, public interest and applicable UK GDPR conditions. Consent is not always required for safeguarding information sharing. Recipients may include local authority safeguarding services, health organisations, police and other authorised agencies as appropriate.
Risk stratification	Purpose: To identify patients at higher risk of deterioration, hospital admission or other adverse outcomes so that preventative or proactive care can be offered and services can be planned. Legal basis: Depends on the current risk-stratification arrangement, including applicable statutory support and UK GDPR conditions. Provider: Existing notice names NHS South, Central and West CSU. DPO / Practice confirmation required for current supplier, legal basis and opt-out arrangements.
SABP / Salus integrated mental health and dementia care	Purpose: To support integrated direct care by enabling authorised Surrey and Borders Partnership staff working within the integrated team to access and record relevant information in the Salus EMIS environment. Legal basis: UK GDPR Article 6(1)(e) and Article 9(2)(h). Controller arrangements: Existing notice states that Salus Medical Services retains controllership for entries made by Salus staff and SABP for entries made by SABP staff. This should be confirmed against the current data-sharing agreement.
Quality monitoring, patient safety concerns and serious incidents	Purpose: To investigate concerns, incidents and quality or safety issues and to support learning and improvement.

	Legal basis: Relevant statutory NHS duties and UK GDPR conditions. Consent is not always required where information must be processed for patient safety, statutory investigation or other lawful governance functions. Recipients may include relevant care providers, NHS bodies, regulators and other public authorities where necessary.
Commissioning, planning, contract monitoring and evaluation	Purpose: To plan, monitor and evaluate health services. Aggregated or anonymous information should be used where identifiable information is not necessary. Legal basis: Applicable statutory NHS functions. Where identifiable information is required, an appropriate lawful and confidentiality basis must be established. Recipients: Current NHS commissioners and contracted support organisations as applicable.
AccuRx Patient Triage	Purpose: To enable patients to submit online consultation and administrative requests and to support Practice communication and triage workflows. Information submitted by a patient may form part of the clinical record where relevant. Legal basis: For care-related use, UK GDPR Article 6(1)(e) and Article 9(2)(h). Other operational processing is governed by the applicable service arrangements. Provider/role: AccuRx. Current processor/controller wording, retention and any international-transfer arrangements should be confirmed against the Practice contract and DPIA.
National registries	Purpose: To support approved national registries, audits and disease surveillance where a lawful authority permits or requires identifiable information to be processed. Legal basis: The specific statutory power, regulation, direction or Section 251 support applicable to the particular registry. Note: The previous blanket statement about all registries having Section 251 approval has been replaced because the legal basis varies by registry.
Care Quality Commission	Purpose: CQC may require access to information where necessary to carry out its statutory regulatory functions. Legal basis: CQC's statutory powers under the Health and Social Care Act 2008 and associated legislation. CQC does not depend on patient consent where it lawfully exercises those powers.
Surveys and patient feedback	Purpose: To obtain feedback and improve services. Legal basis: Depends on the survey and how it is conducted. Participation in optional Practice surveys is voluntary. Where identifiable personal information is collected, the relevant privacy information and lawful basis will be provided.
Research	Purpose: To support appropriately approved health and care research. Legal basis: Varies according to the research project. Consent may be sought for participation or confidentiality where required, but research does not always rely on UK GDPR consent. Other lawful bases, approvals or statutory gateways may apply.
Screening programmes	Purpose: To identify eligible patients and support disease prevention, early diagnosis and screening programmes. Legal basis: Depends on the programme and may include public task and health-care/public-health conditions under UK GDPR, together with applicable confidentiality arrangements. Patients retain choices about participation where the programme provides for this.

Hampshire County Council – Public Health Primary Care Services	Purpose: Richmond Surgery participates in Hampshire County Council commissioned public health services, including NHS Health Checks and Long-Acting Reversible Contraception (LARC). Relevant information is processed where necessary to identify eligible patients, provide the service, maintain clinical records and meet applicable commissioning, monitoring and reporting requirements. Legal basis: UK GDPR Article 6(1)(e) and, where health information is processed, Article 9(2)(h) and/or other applicable public-health conditions depending on the data flow. Current position: NHS Health Checks are delivered under Hampshire County Council's 2026–2033 contract/service specification. LARC is retained as a current commissioned public-health service. DPO confirmation is recommended for commissioner reporting fields and controller roles.
Other organisations providing support services	Purpose: Richmond Surgery may use additional organisations to provide specialist, technical, administrative or clinical support. Legal basis: The lawful basis will depend on the service. Where the organisation acts as a processor, an appropriate contract will govern processing on Richmond Surgery's instructions. Where it acts as a separate controller, information will only be shared where there is an appropriate lawful and confidentiality basis.

Reference Framework

- UK General Data Protection Regulation (UK GDPR), including Articles 13 and 14 transparency requirements.
- Data Protection Act 2018.
- Data (Use and Access) Act 2026, where applicable.
- Common Law Duty of Confidentiality and Caldicott Principles.
- NHS Records Management Code of Practice 2021 and subsequent national guidance.
- Current ICO guidance on the right to be informed and transparency in health and social care.
- Relevant NHS England directions, Data Provision Notices, information standards and data-sharing requirements.

Relevant service contracts, Data Protection Impact Assessments, Data Sharing Agreements and processor contracts held by Richmond Surgery.