

Sherburn & Rillington Practice

Privacy, Confidentiality and Patient Information Policy

Version: 3.0

Policy Owner: Practice Manager

Data Protection Officer: Barry Jackson

Approved by: DPO

Date approved:

Review date:

Applies to: All employees, partners, contractors, locums and individuals working on behalf of Sherburn & Rillington Practice

1. Purpose

Sherburn & Rillington Practice is committed to protecting the privacy, confidentiality and security of personal and confidential information entrusted to us.

This policy explains how the Practice collects, uses, stores, protects and shares personal information and how we provide patients with clear information about the processing of their data.

The Practice processes personal information for a range of purposes, including the provision of direct care, administration of healthcare services, clinical audit, service improvement, research, screening programmes, public health and other purposes permitted or required by law.

The Practice will ensure that personal information is processed fairly, lawfully, transparently and securely.

This policy should be read alongside the Practice's UK GDPR/Data Protection, Confidentiality, Information Governance, Records Management and Information Security policies where applicable.

2. Scope

This policy applies to:

- GP partners;
- salaried and locum GPs;
- nursing and clinical staff;
- dispensary staff;

- reception and administrative staff;
- management;
- PCN staff working within the Practice;
- temporary and agency staff;
- contractors and third parties processing information on behalf of the Practice.

All staff have a responsibility to maintain patient confidentiality and protect personal information.

Every member of staff working within an NHS organisation has a duty to keep information about patients confidential. The existing privacy notice also recognises the Caldicott principle that the duty to share information appropriately for patient care can be as important as the duty to protect confidentiality. PRACTICE PRIVACY NOTICE v6 (1)

3. Legal and Regulatory Framework

The Practice will process personal information in accordance with applicable legislation and guidance, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Common Law Duty of Confidentiality;
- Human Rights Act 1998;
- Health and Social Care Act 2012;
- Freedom of Information Act 2000;
- Gender Recognition Act 2004 where applicable;
- Caldicott Principles;
- NHS information governance and records management requirements.

The Practice will process personal data in accordance with the principles contained within Article 5 UK GDPR and provide privacy information in an appropriate and accessible format. Privacy notice - Practice polic...

4. Data Controller

Sherburn & Rillington Practice is the **Data Controller** for personal information where the Practice determines how and why that information is processed.

As Data Controller, the Practice is responsible for ensuring appropriate measures are in place to protect personal information against:

- unauthorised access;
- unlawful processing;
- accidental loss;
- destruction;
- alteration;
- inappropriate disclosure.

The Practice will maintain appropriate policies, procedures, systems and staff training to protect personal information.

5. Data Protection Officer

The Practice has access to a Data Protection Officer (DPO), who provides advice and support in relation to data protection legislation and information governance.

Data Protection Officer:

[Insert current DPO name/service]

Email:

[Insert]

Telephone:

[Insert]

Patients may contact the Practice or DPO if they have questions or concerns about the way their personal information is processed.

6. Our Privacy Promise

Sherburn & Rillington Practice will:

- keep personal information safe and confidential;
- be open and transparent about how information is used;
- have an appropriate lawful basis for processing information;

- only collect information that is necessary and relevant;
- only use information for appropriate purposes;
- provide patients with information about how their data is used;
- give patients appropriate opportunities to exercise their information rights;
- only share identifiable information where there is an appropriate reason or legal basis;
- maintain appropriate technical and organisational security measures;
- ensure staff receive appropriate confidentiality and information governance training;
- not sell patients' personal information for marketing purposes.

This incorporates the stronger “Privacy Promise” contained within the existing v6 notice.
PRACTICE PRIVACY NOTICE v6 (1)

7. Information We Collect

The Practice collects and processes information necessary to provide healthcare and operate our services.

This may include:

Personal and demographic information

- name;
- date of birth;
- NHS number;
- address;
- telephone number;
- email address;
- next of kin;
- carers;
- legal representatives;
- emergency contacts.

Health and clinical information

- medical history;
- diagnoses;
- consultations;
- appointments;
- medications and prescriptions;
- allergies;
- immunisations;
- test and investigation results;
- referrals;
- hospital correspondence;
- treatment and care plans;
- screening information;
- relevant lifestyle information;
- information received from other health and care professionals.

Other information

Where relevant, the Practice may also process:

- telephone call recordings;
- CCTV images;
- online identifiers;
- information relating to complaints;
- correspondence;
- information required for regulatory or contractual purposes.

The existing Sherburn & Rillington policy specifically identifies recordings of incoming and outgoing Practice telephone calls as information collected by the organisation.

Privacy notice - Practice polic...

8. Why We Use Patient Information

Personal information may be processed for purposes including:

Direct patient care

Information is primarily used to:

- diagnose and treat patients;
- prescribe medication;
- make referrals;
- arrange investigations;
- monitor long-term conditions;
- provide preventative healthcare;
- communicate with other professionals involved in care;
- support continuity of care.

Relevant information may be shared with health or social care professionals where necessary to provide care. For example, information may be included in a hospital referral or provided to a patient's nominated pharmacy. Privacy notice - Practice polic...

Healthcare administration

Information may also be used to:

- manage appointments;
- contact patients;
- manage prescriptions;
- provide recall services;
- process referrals;
- manage correspondence;
- administer Practice services.

Quality, audit and service improvement

Information may be processed to monitor and improve the quality and safety of services.

Public health, screening and preventative care

Information may be processed where necessary to support screening, vaccination, public health and disease prevention programmes.

Planning and research

Information may be processed where there is an appropriate legal basis for healthcare planning, research, audit and service evaluation.

Where possible, anonymised or pseudonymised information will be used.

9. Lawful Basis for Processing

The Practice will identify an appropriate lawful basis under UK GDPR whenever personal data is processed.

Depending upon the purpose, this may include processing necessary:

- for compliance with a legal obligation;
- for the performance of a task carried out in the public interest or exercise of official authority;
- to protect vital interests;
- for the provision and management of healthcare;
- for reasons of public interest in the area of public health;
- for research, statistical or archiving purposes where appropriate;
- where valid consent is the appropriate basis.

Consent is **not automatically the legal basis for all NHS processing**.

For direct care, confidential patient information is generally used within the framework of the Common Law Duty of Confidentiality and appropriate data-protection legislation. The existing notice recognises the use of implied consent for direct patient care while requiring another appropriate justification for non-direct-care processing. PRACTICE PRIVACY NOTICE v6 (1)

10. Confidentiality

All staff must maintain the confidentiality of information obtained during the course of their work.

Access to patient information must be based upon a legitimate need.

Staff must:

- only access information necessary for their role;
- never access records out of curiosity;

- not discuss confidential information where conversations may be overheard;
- protect screens and paper records from unauthorised viewing;
- use approved secure methods of communication;
- comply with Practice information security requirements;
- report suspected confidentiality or data breaches immediately.

Access to electronic patient records is controlled through individual secure user accounts and system access is auditable.

11. Electronic Patient Records

The Practice uses an approved Electronic Patient Record system to maintain patient records.

Electronic records may contain:

- clinical history;
- diagnoses;
- medication;
- allergies;
- investigations and results;
- immunisations;
- correspondence;
- referrals;
- demographic and contact information.

Access must be appropriate to the user's role and responsibilities.

Electronic audit trails may record access and actions undertaken by individual users.

12. Sharing Information for Direct Care

The Practice may share relevant information with health and social care professionals involved in a patient's care.

This may include:

- NHS hospitals and Trusts;

- community services;
- other GP practices;
- pharmacies;
- ambulance services;
- mental health services;
- social care;
- Integrated Care Board services;
- other authorised healthcare providers.

Only information relevant and necessary for the purpose should be shared.

Information may also be disclosed where:

- required by law;
- required by a court;
- necessary to protect vital interests;
- necessary for safeguarding;
- there is another lawful justification for disclosure.

13. Partner Organisations and Data Processors

The Practice uses organisations and systems to support the delivery and administration of healthcare.

Depending on current Practice arrangements, these may include:

- NHS England;
- Humber and North Yorkshire Integrated Care Board;
- NHS Trusts and Foundation Trusts;
- community healthcare providers;
- pharmacies;
- ambulance services;
- local authorities;
- social care organisations;

- NHS-approved IT and clinical system providers;
- Primary Care Network services;
- commissioning/support organisations;
- approved administrative and clinical processing organisations;
- other contracted data processors.

The v6 notice contains particularly useful examples of specific processors, including General Practice Solutions for coding and summarisation, iGPR for report/SAR processing, NHS Account Messaging and Heidi Health for clinical documentation support. PRACTICE PRIVACY NOTICE v6 (1)

The Practice will maintain an up-to-date record of its actual data processors and ensure appropriate contractual/data-processing arrangements are in place.

Where the Practice introduces a new system or processor, the privacy notice will be updated where necessary.

14. Artificial Intelligence and Digital Clinical Tools

Where the Practice uses approved digital or AI-assisted systems, patients will be provided with appropriate information about their use.

For example, where an approved clinical documentation/scribe tool is used, information may be processed to assist a clinician in preparing clinical documentation.

Any draft clinical information generated by such a system must be reviewed appropriately before becoming part of the patient's clinical record.

Relevant systems must be subject to appropriate information governance, data protection and security assessment before implementation.

15. Medicines Management

The Practice may work with authorised medicines management/pharmacy teams to review prescribing and ensure patients receive appropriate, safe and cost-effective treatment.

The existing privacy notice identifies medicines-management support provided through Humber and North Yorkshire Integrated Care Board. PRACTICE PRIVACY NOTICE v6 (1)

Only appropriate information should be accessed for this purpose.

16. Risk Stratification and Population Health Management

Information may be processed to identify patients who may be at increased risk of illness, hospital admission or other adverse health outcomes.

Risk stratification and population health management may help clinicians identify patients who could benefit from preventative interventions or additional support.

Where possible, information will be pseudonymised or anonymised during analysis, with identifiable information only made available where appropriate and necessary.

17. OpenSAFELY

The Practice may participate in nationally authorised data-processing arrangements such as OpenSAFELY.

OpenSAFELY provides a secure environment supporting approved research, clinical audit, service evaluation and health surveillance.

The Sherburn & Rillington policy explains that GP practices remain controllers of their own patient data while approved users may run authorised queries on pseudonymised information without directly accessing identifiable patient information. Privacy notice - Practice polic...

18. National Data Opt-out

Patients have a choice about whether confidential patient information is used for purposes beyond their individual care in circumstances where the National Data Opt-out applies.

The Practice will comply with applicable National Data Opt-out requirements.

Patients should be provided with information explaining how they can view or change their choice.

The National Data Opt-out does **not prevent information being used for the patient's individual care.**

19. Type 1 Opt-out

Where applicable, patients may request a Type 1 Opt-out to prevent confidential patient information being extracted from their GP record for purposes beyond their individual care, subject to applicable exemptions and legal requirements.

Requests should be recorded and processed in accordance with current NHS guidance and the Practice's staff procedure.

20. General Practice Data for Planning and Research

Patient information may be used in accordance with nationally authorised arrangements to support:

- planning health and care services;
- monitoring safety and effectiveness;
- disease prevention;
- research;
- development of treatments;
- improving health services.

The Practice will provide appropriate information to patients about national data collections and available choices.

The existing Sherburn & Rillington policy specifically identifies these purposes within its GDPR section. Privacy notice - Practice polic...

21. CCTV

Where CCTV is operated at Practice premises, its purpose may include:

- safety and security of patients and staff;
- prevention and detection of crime;
- protection of Practice premises.

CCTV footage will be stored securely and access restricted.

Footage may be disclosed where legally appropriate, including to law enforcement agencies.

Individuals may have the right to request footage containing their personal data, subject to the rights of other individuals and applicable exemptions.

Appropriate signage will be displayed where CCTV is in operation.

22. Telephone Call Recording

Where Practice telephone calls are recorded, recordings constitute personal data and will be handled securely.

Call recordings may be used for appropriate purposes including:

- patient care;
- investigation of complaints or incidents;
- staff training and quality assurance;
- protection of patients and staff;
- evidential purposes where appropriate.

Access to recordings will be restricted to authorised staff.

Patients will be provided with appropriate information that calls are recorded.

23. Text Messages, Email and Digital Messaging

The Practice may use approved communication systems to contact patients regarding their healthcare.

This may include:

- SMS/text messages;
- NHS App messaging;
- email where appropriate;
- approved online communication platforms.

Messages may include:

- appointment information;
- recalls;
- health information;
- service updates;
- links to questionnaires;
- other healthcare-related communications.

Staff must take appropriate steps to ensure information is sent to the correct patient/contact details.

Patients should keep their contact information up to date.

The Practice's patient messaging procedure should be followed when sending confidential or sensitive information.

24. Website, Social Media and Cookies

The Practice website may use cookies and similar technologies necessary for functionality and to understand how the website is used.

Where applicable, patients will be provided with information about:

- essential cookies;
- analytical/performance cookies;
- functionality cookies;
- third-party cookies.

The Practice will maintain appropriate privacy information relating to its website and social media presence.

25. Children's Information

Children and young people's personal information will be afforded the same protections as other confidential information.

Information should be provided in an age-appropriate and accessible manner where appropriate.

Consideration should be given to:

- the child's age and understanding;
 - parental responsibility;
 - capacity/competence;
 - confidentiality;
 - safeguarding;
 - the young person's rights.
-

26. Retention of Records

The Practice will retain health and administrative records in accordance with applicable NHS Records Management requirements.

Records must not be retained longer than necessary unless there is a legal, regulatory or clinical justification for continued retention.

Records reaching the end of their retention period must be reviewed and securely disposed of where appropriate.

The Practice should maintain a records retention schedule aligned with current NHS requirements.

27. Patient Rights

Subject to applicable exemptions and limitations, individuals have rights regarding their personal data, including the right to:

- be informed about how their information is used;
- request access to their information;
- request correction of inaccurate information;
- request erasure in certain circumstances;
- request restriction of processing in certain circumstances;
- object to certain processing;
- data portability where applicable;
- raise concerns about the use of their information.

These rights do not mean that a patient can automatically require their medical record to be deleted.

The Practice may need to retain information where there is a legal, contractual, regulatory or clinical requirement.

28. Subject Access Requests

Patients have the right to request access to personal information held about them.

Requests may be made verbally or in writing.

The Practice must take reasonable steps to verify the identity of the person making the request.

Subject Access Requests will normally be completed within **one month**, subject to the provisions allowing an extension for particularly complex requests.

Information should normally be supplied without charge, although data protection legislation permits fees or refusal in limited circumstances involving manifestly unfounded or excessive requests.

The existing v6 notice contains detailed patient guidance on access, rectification, erasure and response times. PRACTICE PRIVACY NOTICE v6 (1)

29. Data Accuracy

The Practice will take reasonable steps to ensure personal information is accurate and kept up to date.

Patients should be encouraged to notify the Practice when their:

- address;
- telephone number;
- email address;
- name;
- next of kin/contact information

changes.

Requests to amend clinical information should be handled in accordance with the Practice's records management procedures.

30. Information Security

Appropriate technical and organisational measures will be used to protect information.

These include, where appropriate:

- individual user accounts;
- role-based access;
- strong authentication;
- audit trails;
- secure NHS-approved systems;
- secure email;
- physical security;

- staff confidentiality agreements;
 - information governance training;
 - secure disposal;
 - incident and breach management procedures.
-

31. Personal Data Breaches

Any actual or suspected loss, inappropriate disclosure, unauthorised access or other breach involving personal information must be reported immediately through the Practice's incident reporting process.

The Practice Manager/Data Protection Lead will assess the incident and obtain DPO advice where appropriate.

Reportable incidents will be managed in accordance with applicable data protection and NHS requirements.

32. Complaints and Concerns

Patients who have concerns about how their personal information has been managed should contact the Practice in the first instance.

Practice Manager

Sherburn & Rillington Practice

[Insert current contact details]

Patients may also contact the Practice's Data Protection Officer.

Where a patient remains dissatisfied, they have the right to raise their concern with the **Information Commissioner's Office (ICO)**.

33. Accessible Privacy Information

The Practice recognises that patients may require information in alternative formats or additional support to understand how their information is used.

Privacy information should be made available in accessible formats where reasonably required.

Patients should be encouraged to inform the Practice if they require:

- an interpreter;

- translation;
 - Easy Read information;
 - large print;
 - communication support;
 - another reasonable adjustment.
-

34. Staff Responsibilities

All staff must:

- maintain confidentiality;
- only access information required for their role;
- follow information governance and data protection procedures;
- complete mandatory training;
- report breaches promptly;
- use approved systems;
- ensure information is shared securely and appropriately.

Practice Manager / Data Protection Lead

Responsible for:

- maintaining this policy;
- ensuring the Privacy Notice remains current;
- ensuring appropriate staff training;
- maintaining information governance processes;
- ensuring new processors/systems are assessed;
- coordinating responses to data protection incidents;
- liaising with the DPO.

Data Protection Officer

Provides independent advice and support regarding data protection compliance and associated risks.

35. Training

All staff must undertake appropriate:

- data security awareness training;
- confidentiality training;
- information governance training;
- additional training relevant to their responsibilities.

Information governance requirements should form part of staff induction.

36. Monitoring and Review

The Practice will periodically review its information governance arrangements.

This should include consideration of:

- whether the Privacy Notice remains accurate;
- changes to data processors;
- new digital systems;
- changes to data-sharing arrangements;
- information governance incidents;
- Subject Access Requests;
- complaints relating to confidentiality;
- changes to legislation or national guidance.

The policy will be reviewed at least annually or sooner where there is a significant change.

Annex A – Patient Privacy Notice

How Sherburn & Rillington Practice uses your information

Sherburn & Rillington Practice has a legal duty to explain how we use the personal and healthcare information we collect about you.

We maintain records about your health and the care you receive. These records may be electronic or paper based.

We use your information primarily to provide you with safe and effective healthcare.

We may also use information where appropriate for:

- managing our services;
- clinical audit;
- improving quality and safety;
- screening and preventative care;
- public health;
- planning NHS services;
- authorised research;
- meeting our legal and regulatory obligations.

Where appropriate, relevant information may be shared with other health and social care professionals involved in your care.

We will only use and share information where there is an appropriate reason and lawful basis for doing so.

You have rights regarding your personal information, including the right to request access and correction of inaccurate information.

You can also make choices about certain uses of confidential patient information beyond your individual care through applicable NHS data opt-out arrangements.

If you have questions about how we use your information, please contact the Practice Manager or our Data Protection Officer.

Annex B – Practice Data Processors and Information Sharing Register

The Practice will maintain a separate, controlled register of organisations with which information is routinely shared or which process information on behalf of the Practice.

The register should record:

Organisation/System	Purpose	Information shared/accessed	Controller/Processor	Legal basis/authority	DSA/DPA/contract	Review date
TPP/SystemOne	Electronic patient record	Patient/clinical information	Processor	Healthcare provision	In place	Annual
Humber & North Yorkshire ICB	Commissioning/clinical services	Relevant patient information	As applicable	NHS functions	Review	Annual
NHS Trusts	Direct care	Relevant clinical information	Controller-to-controller	Direct care	As applicable	Annual
Community Services	Direct care	Relevant clinical information	Controller-to-controller	Direct care	As applicable	Annual
General Practice Solutions	Coding/summarisation	Relevant clinical records	Processor	Contracted service	Confirm	Annual
iGPR	Reports/SAR support	Relevant patient information	Processor	Contracted service	Confirm	Annual

Organisation/System	Purpose	Information shared/accessed	Controller/Processor	Legal basis/authority	DSA/DPA/contract	Review date
[AI/Scribe provider if used]	Clinical documentation	Relevant consultation information	Processor	Healthcare provision	DPIA/DPA	Annual
NHS England messaging services	Patient communication	Contact/health information	As applicable	NHS functions	As applicable	Annual

This register must reflect the systems and organisations actually used by Sherburn & Rillington Practice and should be reviewed whenever a new processor or data-sharing arrangement is introduced.

Annex C – Patient Messaging

Before sending patient information electronically, staff must:

1. Confirm the correct patient.
 2. Check current contact details.
 3. Use an approved Practice system.
 4. Consider the sensitivity of the information.
 5. Check any recorded communication preferences or reasonable adjustments.
 6. Ensure messages contain only the information necessary.
 7. Record communication appropriately within the patient record.
-

Annex D – Data Opt-out Staff Procedure

When a patient asks about use of their information for purposes beyond their individual care:

1. Establish whether their query relates to a **Type 1 Opt-out, National Data Opt-out**, or general information sharing.
 2. Provide appropriate current patient information.
 3. Do not advise the patient that opting out prevents information being shared for their direct healthcare.
 4. Process Type 1 requests according to the Practice's clinical system procedure.
 5. Signpost patients appropriately for National Data Opt-out choices.
 6. Record relevant correspondence/actions.
 7. Escalate complex queries to the Practice Manager/Data Protection Lead or DPO.
-

Annex E – Privacy Notice Publication Checklist

The Practice will ensure that:

- ☐ Full Privacy Notice is available on the Practice website
- ☐ Privacy information is displayed/signposted within both Practice sites
- ☐ Patients can request a paper copy
- ☐ Accessible formats are available where required
- ☐ Current DPO details are published

- ☐ Current Practice contact details are published
 - ☐ Current processors are reflected within privacy information
 - ☐ New systems/processors trigger a privacy review
 - ☐ Staff know where to direct patient privacy queries
 - ☐ Privacy Notice is reviewed at least annually
-

Approved by: _____

Date: _____

Next review: _____

Version: _____