Hastings & Rother Healthcare

Be Committed
Be Caring
Be Excellent

Hastings & Rother Healthcare

Privacy Notice

Our contact details:

Name: Hastings & Rother Healthcare

Address: The Ice House, Rock-a-Nore, Hastings, TN34 3DW

Phone Number: 01424 452 800

E-mail: sxicb-esx.hastingsoldtownsurgery@nhs.net

Fair Processing Notice (Privacy Notice)

YOUR INFORMATION, WHAT YOU NEED TO KNOW:

This privacy notice explains why we collect information about you, how that information will be used, how we keep it safe and confidential and what your rights are in relation to this.

WHY WE COLLECT INFORMATION ABOUT YOU:

Health care professionals who provide you with care are required by law to maintain records about your health and any treatment or care you have received. These records help to provide you with the best possible healthcare and help us to protect your safety.

We collect and hold data for the purpose of providing healthcare services to our patients and running our organisation which includes monitoring the quality of care that we provide. In carrying out this role we will collect information about you which helps us respond to your queries or secure specialist services. We will keep your information in written form and/or in digital form

Updated: June 2026

Hastings & Rother Healthcare

Be Committed
Be Caring
Be Excellent

OUR COMMITMENT TO DATA PRIVACY AND CONFIDENTIALITY ISSUES

As a GP practice, all of our GPs, staff and associated practitioners are committed to protecting your privacy and will only process data in accordance with the Data Protection Legislation. This includes the General Data Protection Regulation (EU) 2016/679 (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time. The legislation requires us to process personal data only if there is a legitimate basis for doing so and that any processing must be fair and lawful.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

DATA WE COLLECT ABOUT YOU:

Records which this GP Practice will hold or share about you will include the following:

- Personal Data – means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- Special Categories of Personal Data – this term describes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- Confidential Patient Information – this term describes information or data relating to their health and other matters disclosed to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. Including both information 'given in confidence' and 'that which is owed a duty of confidence'. As described in the Confidentiality: NHS code of Practice: Department of Health guidance on confidentiality 2003.

- Pseudonymised – The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.

- Anonymised – Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place

- Aggregated – Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

HOW WE USE YOUR INFORMATION

Improvements in information technology, including secure online triage, appointment and communication systems, are making it possible for us to share data with other healthcare organisations for the purpose of providing you, your family and your community with better care. For example it is possible for healthcare professionals in other services to access your record with your permission when the practice is closed. This is explained further in the Local Information Sharing at Appendix A.

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment. The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

A full list of details including the legal basis, any Data Processor involvement and the purposes for processing information can be found in Appendix A.

HOW LONG DO WE HOLD INFORMATION FOR?

All records held by the Practice will be kept for the duration specified by national guidance from NHS Digital, Health and Social Care Records Code of Practice. Once information that we hold has been identified for destruction it will be disposed of in the most appropriate way for

the type of information it is. Personal confidential and commercially confidential information will be disposed of by approved and secure confidential waste procedures. We keep a record of retention schedules within our information asset registers, in line with the Records Management Code of Practice for Health and Social Care 2016.

USE OF AI SCRIBES IN CONSULTATIONS

As part of our commitment to improving the quality of care and reducing administrative time during appointments, we have introduced the choice of patients opting for the use of an AI scribe tool provided by Tandem Health. This is not a requirement and patients will be asked for their preference when their face to face appointment begins.

During your consultation, the AI scribe listens in real-time and produces a written summary of the conversation for your clinician. This means your clinician can focus fully on listening to you and your needs, rather than typing notes during the appointment.

What This Means for You:

- Your care remains unchanged – the clinician still makes all the necessary clinical decisions.
- All AI scribed notes are reviewed and approved by the clinician before being saved in your medical record to ensure accuracy.
- You the patient, benefit from more complete and accurate notes.

How Your Privacy is Protected:

We take your privacy and data protection very seriously. The use of Tandem Health complies with strict NHS and GDPR data security standards.

- The audio of your consultation is never stored. It is transcribed in real-time and then immediately deleted.
- No personal information (e.g., name, NHS number, date of birth) is stored or processed by the AI system.
- Notes are securely encrypted and stored in accordance with ISO 27001 and NHS Digital's Data Security and Protection Toolkit (DSPT) standards.
- All data is processed within Microsoft Azure's secure data centre, under robust enterprise-level security agreements.
- Tandem Health does not train its AI models using patient data.
- Regular external penetration testing is carried out to ensure system security.

Tandem Health AI is also Cyber Essentials certified and operates independently of your medical record system, meaning no explicit link is made between the transcript and your personal details within the AI platform.

Updated: June 2026

Hastings & Rother Healthcare

Be Committed
Be Caring
Be Excellent

USE OF RAPID HEALTH ONLINE TRIAGE AND APPOINTMENT SYSTEM

As part of our commitment to improving access to care and reducing waiting times, Hastings & Rother Healthcare uses the Rapid Health online triage and appointment system.

Rapid Health allows patients to:

- submit medical and administrative requests online,
- receive signposting to appropriate NHS services,
- book certain appointments online where appropriate,
- request repeat prescriptions, fit notes and other administrative support,
- provide information to help the practice prioritise care safely and effectively.

The system works using pre-configured clinical and administrative rules set by the practice. Depending on the information entered, patients may:

- be offered self-care advice,
- be directed to another NHS service,
- be invited to book an appointment,
- or have their request reviewed by the practice team.

The information submitted through Rapid Health is shared securely with the practice and may be added to your medical record.

Important Information About Automated Processing

Rapid Health uses automated workflow technology to support appointment prioritisation and navigation through practice services. However:

- the system does not replace clinical judgement,
- no fully automated clinical decisions are made about your care,
- and clinicians and practice staff remain responsible for reviewing requests and making decisions regarding treatment and care.

Rapid Health does not use generative AI or large language models to make clinical decisions.

How Your Information is Protected

Rapid Health operates in accordance with UK GDPR and NHS data security standards. Data is:

- encrypted in transit and at rest,
- hosted within secure UK-based infrastructure,
- protected through role-based access controls,
- and processed under formal data processing agreements.

Updated: June 2026

Rapid Health is compliant with the NHS Data Security and Protection Toolkit (DSPT) and Cyber Essentials standards.

Patients may access Rapid Health using details matched against the practice clinical system and, where enabled, NHS Login authentication.

Retention of Information
Information submitted through Rapid Health is retained within the practice clinical record in accordance with NHS Records Management requirements.

Requests temporarily held within the Rapid Health Smart Inbox are retained for a limited period before deletion:

- Medical Requests – up to two weeks after processing
- Administrative Requests – up to two weeks after processing

Use of Outsourced Medical Reporting Services

We may use specialist NHS-approved medical reporting providers to support the production of Subject Access Requests (SARs), insurance reports, occupational health reports and other authorised medical reports. These providers act on our instructions as Data Processors and are contractually required to comply with UK GDPR, the Data Protection Act 2018 and NHS information governance requirements. Patient information is only processed where there is an appropriate legal basis and, where required, patient consent.

TELEPHONE CALL RECORDS

The telephone call recording system in operation will record incoming and outgoing telephone calls. All telephone calls received into the practice will be summarised and added to patient's record to allow provision of the highest level of care for the patient. All call recordings are encrypted and stored on a secure server.

Telephone call recordings will be retained by HRH for 30 days and will not be held longer than 30 days, unless it is subject to a form of access request for example Subject Access Request (SAR). If an individual should request their clinical and non-clinical call recordings as part of a SAR, they will be provided with a transcription of the call. Before handing over the information, the call recording will undergo redaction according to the organisational process.

Where the information is considered to be sensitive, especially around information that may cause harm, the information should be prepared as per SAR request process and then, the individual should be offered a meeting with a clinician to discuss the entry prior to handing over the information in order to reduce any possible harm.

INDIVIDUALS RIGHTS UNDER GDPR

Under GDPR 2016 the Law provides the following rights for individuals. The NHS uphold these rights in a number of ways.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure (not an absolute right) only applies in certain circumstances
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

YOUR RIGHT TO OPT OUT OF DATA SHARING AND PROCESSING

The NHS Constitution states 'You have a right to request that your personal and confidential information is not used beyond your own care and treatment and to have your objections considered'.

Type 1 Opt Out

This is an objection that prevents an individual's personal confidential information from being shared outside of their general practice except when it is being used for the purposes of direct care, or in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease. If patients wish to apply a Type 1 Opt Out to their record they should make their wishes know to the practice manager.

National data opt-out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt-out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

By 2020 all health and care organisations are required to apply national data opt-outs where confidential patient information is used for research and planning purposes. NHS Digital has been applying national data opt-outs since 25 May 2018. Public Health England has been applying national data opt-outs since September 2018.

The national data opt-out replaces the previous 'type 2' opt-out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care. Any patient that had a type 2 opt-out recorded on or before 11 October 2018 has had it automatically converted to a national data opt-out. Those aged 13 or over were sent a letter

giving them more information and a leaflet explaining the national data opt-out. For more information go to National data opt out programme

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters.

On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service.

NHS England has been directed by the government to establish and operate the OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service. These services provide a secure environment that supports research, clinical audit, service evaluation and health surveillance for COVID-19 and other purposes.

Each GP practice remains the controller of its own GP patient data but is required to let approved users run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym.

Only approved users are allowed to run these queries, and they will not be able to access information that directly or indirectly identifies individuals.

Patients who do not wish for their data to be used as part of this process can register type 1 opt out with their GP.

Find additional information about OpenSAFELY.

RIGHT OF ACCESS TO YOUR INFORMATION (SUBJECT ACCESS REQUEST)

Under Data Protection Legislation everybody has the right to have access to, or request a copy of, information we hold that can identify you, this includes your medical record, there are some safeguards regarding what you will have access and you may find information has been redacted or removed for the following reasons;

- Does not cause harm to the patient
- That legal confidentiality obligations for the non-disclosure of third-party information are adhered to

You do not need to give a reason to see your data and requests can be made in writing. We may ask you to complete a form in order that we can ensure that you have the correct information you require.

Where multiple copies of the same information is requested the surgery may charge a reasonable fee for the extra copies.

You will need to provide proof of identity to receive this information.

If you would like to access your GP record online please ask a member of our reception team.

CHANGE OF DETAIL

It is important that you tell the surgery if any of your contact details such as your name or address have changed especially if any of your other contacts details are incorrect. It is important that we are made aware of any changes **immediately** in order that no information is shared in error.

MOBILE TELEPHONE NUMBER

If you provide us with your mobile phone number, we may use this to send you text reminders about your appointments or other health screening information. Please let us know if you do not wish to receive text reminders on your mobile.

EMAIL ADDRESS

Where you have provided us with your email address, with your consent we will use this to send you information relating to your health and the services we provide. If you do not wish to receive communications by email please let us know.

NOTIFICATION

Data Protection Legislation requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information.

We are registered as a Data Controller and our registration can be viewed online in the public register at: http://ico.org.uk/what_we_cover/register_of_data_controllers

Any changes to this notice will be published on our website and in a prominent area at the Practice.

DATA PROTECTION OFFICER

Should you have any data protection questions or concerns, please contact: sxicb-esx.hastingsoldtownsurgery@nhs.net

Our current DPO is Laura Taw.

WHAT IS THE RIGHT TO KNOW?

The Freedom of Information Act 2000 (FOIA) gives people a general right of access to information held by or on behalf of public authorities, promoting a culture of openness and accountability across the public sector. You can request any non-personal information that the GP Practice holds, that does not fall under an exemption. You may not ask for information that is covered by the Data Protection Legislation under FOIA. However you can request this under a right of access request – see section above 'Access to your information'.

RIGHT TO COMPLAIN

If you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, please contact the practice via our Patient Liaison Officer at the following contact details:

sxicb-esx.hrh.patientliaison@nhs.net;

If you are not happy with our responses and wish to take your complaint to an independent body, you have the right submit a complaint with the Information Commissioner's Office.

You can contact them by calling: 0303 123 1113

Or go online to https://ico.org.uk/global/contact-us

The Information Commissioner's Office address is:

Hastings & Rother Healthcare

Be Committed
Be Caring
Be Excellent

Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

THE NHS CARE RECORD GUARANTEE

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS, what control the patient can have over this, the rights individuals have to request copies of their data and how data is protected under Data Protection Legislation.

http://systems.digital.nhs.uk/infogov/links/nhscrg.pdf

THE NHS CONSTITUTION

The NHS Constitution establishes the principles and values of the NHS in England. It sets out the rights patients, the public and staff are entitled to. These rights cover how patients access health services, the quality of care you'll receive, the treatments and programs available to you, confidentiality, information and your right to complain if things go wrong.

https://www.gov.uk/government/publications/the-nhs-constitution-for-england

APPENDIX A :

THE PRACTICE WILL SHARE YOUR INFORMATION WITH THESE ORGANISATIONS WHERE THERE IS A LEGAL BASIS TO DO SO.

ICB	**Purpose –** Anonymous data is used by the ICB for planning and performance as directed in the practices contract. **Legal Basis** – Contractual **Processor** – East Sussex ICB
Summary Care Records	**Purpose –** Practices have been told to share details of patients personal confidential and special category data onto the summary care record. The NHS in England uses a national electronic record called the Summary Care Record (SCR) to support patient care. It contains key information from your GP record. Your SCR provides authorised healthcare staff with faster, secure access to essential information about you in an emergency or when you need unplanned care, where such information would otherwise be unavailable. **Legal Basis** – Direct Care The relevant COPI notice states that its purpose: "…is to require organisations to process confidential patient information for the purposes set out in Regulation 3(1) of COPI to support the Secretary of State's response to Covid-19 (Covid-19 Purpose). "Processing" for these purposes is defined in Regulation 3(2) and includes dissemination of confidential patient information to persons and organisations permitted to process confidential patient information under Regulation 3(3) of COPI." Full details of the Summary Care Record supplementary privacy notice can be found here Patients have the right to opt out of having their information shared with the SCR by completion of the form which can be downloaded here and returned to the practice. Please note that by opting out of having your information shared with the Summary Care Record could result in a delay care that may be required in an emergency. **Processor –** NHS England and NHS Digital via GP connect,
Research	**Purpose –** We many share personal confidential or anonymous information with research companies. Where you have opted

	out of having your identifiable information shared for this purpose your information will be removed. **Legal Basis –** consent is required to share confidential patient information for research, unless there is have support under the Health Service (Control of Patient Information Regulations) 2002 ('section 251 support') applying via the Confidentiality Advisory Group in England and Wales **Processor –** N/A at this time
Individual Funding Requests	**Purpose –** We may need to process your personal information where we are required to fund specific treatment for you for a particular condition that is not already covered in our contracts. **Legal Basis –** The clinical professional who first identifies that you may need the treatment will explain to you the information that is needed to be collected and processed in order to assess your needs and commission your care; they will gain your explicit consent to share this. You have the right to withdraw your consent at any time
Safeguarding Adults	**Purpose –** We will share personal confidential information with the safeguarding team where there is a need to assess and evaluate any safeguarding concerns. **Legal Basis –** Because of public Interest issues, e.g. to protect the safety and welfare of vulnerable adults, we will rely on a statutory basis rather than consent to process information for this use.
Safeguarding Children	**Purpose –** We will share children's personal information where there is a need to assess and evaluate any safeguarding concerns.

	Legal Basis – Because of public Interest issues, e.g. to protect the safety and welfare of Safeguarding we will rely on a statutory basis rather than consent to share information for this use.
Risk stratification – preventative Care	**Purpose –** 'Risk stratification for case finding' is a process for identifying and managing patients who have or may be at-risk of health conditions (such as diabetes) or who are most likely to need healthcare services (such as people with frailty). Risk stratification tools used in the NHS help determine a person's risk of suffering a particular condition and enable us to focus on preventing ill health before it develops. Information about you is collected from a number of sources including NHS Trusts, GP Federations and your GP Practice. A risk score is then arrived at through an analysis of your de-identified information. This can help us identify and offer you additional services to improve your health. If you do not wish information about you to be included in any risk stratification programmes, please let us know. We can add a code to your records that will stop your information from being used for this purpose. Please be aware that this may limit the ability of healthcare professionals to identify if you have or are at risk of developing certain serious health conditions. Type of Data – Identifiable/Pseudonymised/Anonymised/Aggregate Data **Legal Basis** - GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of identifiable data by ICBs and GPs for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-04)(a)/2013)) and this approval has been extended to the end of September 2020 NHS England Risk Stratification which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for risk stratification purposes which sets aside the duty of confidentiality. We are committed to conducting risk stratification effectively, in ways that are consistent with the laws that protect your confidentiality.

Public health : screening programme (identifiable), notifiable disease information (identifiable), smoking cessation (anonymous), sexual health (anonymous)	**Purpose –** Personal identifiable and anonymous data is shared. The NHS provides national screening programmes so that certain diseases can be detected at an early stage. These currently apply to bowel cancer, breast cancer, aortic aneurysms and diabetic retinal screening service. The law allows us to share your contact information with Public Health England so that you can be invited to the relevant screening programme. More information can be found at: https://www.gov.uk/topic/population-screeningprogrammes [Or insert relevant link] or speak to the practice **Legal Basis –** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below **Data Processors** – Public Health England
Direct care, NHS trusts, other care providers , Community Pharmacist Consultation Service, Pharmacy First, One you, Primary Care Hub – ic24	**Purpose** – Personal information is shared with other secondary care trusts in order to provide you with direct care services. This could be hospitals or community providers for a range of services, including treatment, operations, physio, and community nursing, ambulance service. **Legal Basis** – The processing of personal data in the delivery of direct care and for providers' administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 and 9 conditions as stated below: **Processors** – East Sussex Healthcare NHS Trust Sussex Partnership NHS Foundation Trust
Care Quality Commission	**Purpose** – The CQC is the regulator for the English Health and Social Care services to ensure that safe care is provided. They will

	inspect and produce reports back to the GP practice on a regular basis. The Law allows the CQC to access identifiable data. More detail on how they ensure compliance with data protection law (including GDPR) and their privacy statement is available on our website: https://www.cqc.org.uk/about-us/our-policies/privacy-statement **Legal Basis** – Article 6(1)(c) "processing is necessary for compliance with a legal obligation to which the controller is subject." And Article 9(2) (h) as stated below **Processor**s – Care Quality Commission
Emotional Wellbeing Service and Severe Mental Illness (SMI) Support Service	**Purpose** – Personal and special category health information may be shared with Sussex Partnership NHS Foundation Trust (SPFT) to provide direct mental health care and support services. This will only be patients on the Severe Mental Illness (SMI) specific health registers/searches. This includes assessment, treatment, care planning, emotional wellbeing support, Severe Mental Illness (SMI) physical health checks, referrals to specialist mental health services and the recording of consultations to support the ongoing care of patients. **Legal Basis** – 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 Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'. **Processor / Data Sharing Partner** – Sussex Partnership NHS Foundation Trust (SPFT) **Categories of Data Processed** – This may include: • Patient demographic information • NHS Number • Medical records • Clinical documentation • Consultation records

	• Mental health assessments • Medications • Clinical problems and diagnoses • Test results • Social and family history • Referral information Information is shared solely for the provision of direct healthcare. Consultations may be recorded within both GP clinical systems and SPFT clinical systems where necessary for the provision of care. Information may also be used in anonymised or aggregated form for healthcare service planning, reporting and service improvement purposes.
Payments, invoice validation	Purpose – Contract holding GPs in the UK receive payments from their respective governments on a tiered basis. Most of the income is derived from baseline capitation payments made according to the number of patients registered with the practice on quarterly payment days. These amount paid per patient per quarter varies according to the age, sex and other demographic details for each patient. There are also graduated payments made according to the practice's achievement of certain agreed national quality targets known as the Quality and Outcomes Framework (QUOF), for instance the proportion of diabetic patients who have had an annual review. Practices can also receive payments for participating in agreed national or local enhanced services, for instance opening early in the morning or late at night or at the weekends. Practices can also receive payments for certain national initiatives such as immunisation programs and practices may also receive incomes relating to a variety of non patient related elements such as premises. Finally there are short term initiatives and projects that practices can take part in. Practices or GPs may also receive income for participating in the education of medical students, junior doctors and GPs themselves as well as research. In order to make patient based payments basic and relevant necessary data about you needs to be sent to the various payment services. The release of this data is required by English laws.

	Legal Basis – Article 6(1)(c) "processing is necessary for compliance with a legal obligation to which the controller is subject." And Article 9(2)(h) 'as stated below **Data Processors** – NHS England, ICB, Public Health
Patient Record Database/Integrated Health & Care System	**Purpose –** Your medical record will be shared, in order that a data base can be maintained and managed in a secure way and provide Practitioners with right information at the right time. In addition to consultations, the following information can be seen: • Diagnoses • Investigations Results/Observations • Immunisations • Information to inform emergency care delivery • Frailty Assessment • Allergies and Adverse Reactions • Medications **Legal Basis –** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below **Processor** – EMIS, EMIS ESearcher, Plexus Care Record
Medical Reports/Subject Access Requests (Medi2data)	**Purpose -** Hastings & Rother Healthcare uses Medidata Exchange Limited ("Medi2data") to assist with the management and fulfilment of: • Subject Access Requests (SARs) • Insurance reports • Occupational health reports • Department for Work and Pensions (DWP) reports • Ministry of Defence (MoD) reports • Ministry of Justice (MoJ) reports • Other authorised third-party medical reporting requests Medi2data supports the practice by securely extracting, reviewing, redacting and disclosing relevant patient

	information where there is an appropriate legal basis and, where required, patient consent. Medi2data may also provide patients with secure online access to records and reports through a protected patient portal. All disclosures remain subject to appropriate clinical review, redaction processes and governance controls. **Legal Basis -** The processing of personal data is carried out under: • UK GDPR Article 6(1)(e) – Public Task • UK GDPR Article 9(2)(h) – Management of Health and Social Care Systems and Services Where reports are produced for insurers, employers or other third parties, processing may additionally rely upon: • Article 6(1)(a) – Consent • Article 6(1)(b) – Contract where appropriate. **Processor -** Medidata Exchange Limited (Medi2data) ICO Registration Number: ZA353121 DSP Toolkit Organisation Code: 8JQ49 **Categories of Data Processed -** This may include: • Patient demographic information • NHS Number • Medical records • Consultation history • Clinical correspondence • Referral information • Investigation results • Reports and supporting documentation Only information relevant to the specific request will be processed. **International Transfers -** Medi2data uses authorised personnel employed by its wholly owned subsidiary,

	Medi2data SA (Pty) Ltd, in South Africa to support aspects of medical reporting and clinical review services. Where access to patient information occurs from South Africa: • Data remains hosted within secure UK or EU infrastructure. • Access is restricted to authorised personnel. • Appropriate contractual safeguards are in place. • International transfers are protected through the UK International Data Transfer Agreement (IDTA) and associated transfer safeguards. No automated decision-making or profiling is undertaken as part of this service. **Retention -** Reports and associated information are retained in accordance with NHS Records Management requirements and Medi2data contractual retention schedules.
MedLink Patient Recall and Review System	**Purpose** – Personal and special category health information is processed through the MedLink Patient Recall and Review System to support the management of long-term conditions and preventative healthcare. The system reviews information held within the patient record to identify when reviews, tests or assessments may be due and enables patients to complete online questionnaires and reviews. Information provided by patients is reviewed by practice staff before being incorporated into the clinical record. **Legal Basis** – 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 Article 9(2)(h) 'processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'. **Processor** – MedLink Solutions

	Categories of Data Processed – This may include: • Patient demographic information • NHS Number • Medical records • Clinical conditions and diagnoses • Long-term condition review information • Questionnaire responses • Test and monitoring results • Medication information • Appointment and consultation information Information submitted by patients is reviewed by authorised practice staff before being added to the patient record. Anonymous usage information may be used to provide service management information and reporting.
Medicines Optimisation	Purpose – Your anonymous aggregated information will be shared in order to optimise medication. This will enable your GP to provide a more efficient medication regime for your personal care. Some of the anonymous information may be used nationally to drive wider understanding of the medication is used. No patients will be able to identified from the data shared. Legal Basis – Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below Processor – ICB Medicines Management Team
Medicines Management Team	Purpose – your medical record is shared with the medicines management team, in order that your medication can be kept up to date and any changes can be implemented. Legal Basis – Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below

	Processor – ICB Medicines Management Team
GP Federation, GP extended access, video consultations , minor injuries services	**Purpose –** Your medical record will be shared with the Hastings PCN in order that they can provide direct care services to the patient population. This could be in the form of video consultations, Minor injuries clinics, GP extended access clinics **Legal Basis** – Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below **Processor** – Hastings PCN
Smoking Cessation	**Purpose –** personal information is shared in order for the smoking cessation service to be provided. **Legal Basis –** consented **Processor –** OneYou, Southdowns
Social prescribers	**Purpose** – Access to medical records is provided to social prescribers to undertake a full service to patients dependent on their social care needs. **Legal Basis** – Consented **Processor –** Southdowns
Medical Reports	**Purpose –** Personal information will be shared with Insurance companies, or potential or active employers at the patients request **Legal Basis –** Consented

	Processor – Patients and or their representatives – e.g. Insurance companies, RAF, Navy
Police	**Purpose –** Medical reports may be requested by the police for criminals **Legal Basis –** Consented or Article 10 GDPR **Processor –** Police Constabulary
Coroners	**Purpose –** Personal information may be shared with the coroner **Legal Basis –** Legal Obligation **Processor –** The Coroner
Private Healthcare Providers	**Purpose –** Personal information shared with private health care providers in order to deliver direct care to patients at the patients request **Legal Basis –** Consented and under contract between the patient and the provider **Provider** – Private healthcare
Texting service	**Purpose –** Personal identifiable information shared with the texting service in order that text messages including appointment reminders, campaign messages related to specific patients health needs and direct messages to patients **Legal Basis –** Consent from patients and direct care **Provider –** AccuRX, NHS App Hastings & Rother Healthcare use the NHS Account Messaging Service provided by NHS Digital to send you messages relating to your health and care. You need to be an NHS App user to receive these messages. Further information about the service can be found at the privacy notice for the NHS App managed by

	NHS Digital at: https://www.nhs.uk/using-the-nhs/nhs-services/the-nhs-app/privacy/"
Remote consultation: including – video consultation , clinical photography	**Purpose** – Personal information including images may be processed, stored and with the patients consent shared, in order to provide the patient with urgent medical advice. **Legal Basis –** Direct Care and Consent Patients will be asked to provide consent if required to provide photographs of certain areas of concern. There are restrictions on what the practice can accept photographs of. No photographs of the full face, no intimate areas, no pictures of patients who cannot consent to the process. No pictures of children. **Processor –** Rapid Health, AccuRX
Rapid Health Online Triage and Appointment System	**Purpose** – Personal and special category health information is processed through the Rapid Health online triage and appointment system to support: • online medical and administrative requests, • appointment prioritisation, • patient self-booking, • signposting to appropriate NHS services, • remote consultations where appropriate, • and the management of patient enquiries and requests. Information submitted by patients may be reviewed by clinicians and practice staff and added to the patient medical record where appropriate. **Legal Basis –** Article 6(1)(e) – "necessary in the exercise of official authority vested in the controller" and Article 9(2)(h) – "management of health or social care systems and services". **Processor –** Rapid Health Ltd

	NHS login If you access Rapid Health using your NHS login details, the identity verification services are managed by NHS England. NHS England is the controller for any personal information you provided to NHS England to get an NHS login account and verify your identity and uses that personal information solely for that single purpose. For this personal information, our role is a "data processor" only and we must act under the instructions provided by NHS England (as the "data controller") when verifying your identity. For more information on NHS login, see the NHS login privacy notice and NHS login terms and conditions. **NHS App** You can access Rapid Health on the NHS App using your NHS login details. If you sign in using NHS login, we will ask your permission to share your NHS login information with our service. This allows us to fill in some personal details for you, such as your name, date of birth and contact details. We will not use your NHS login information for any other purposes. You can only share your NHS login information if you have proved your identity to NHS login. You can choose not to share your NHS login information with Rapid Health but you will need to enter your information yourself whilst using the service. For more information, see the NHS login privacy notice and NHS login terms and conditions.
MDT Meetings	**Purpose** – Personal information will be discussed with other providers of care, in order to provide a secure video meeting platform to discuss patients. **Legal Basis –** Direct Care **Processor –** MS Teams

Covid- 19 Research and Planning	Purpose – for the collection of Personal confidential data regarding the diagnosis, testing, self-isolating, fitness to work, treatment medical and social interventions and recovery from Covid-19. To enable research and planning during the Covid-19 pandemic. Legal Basis – Notice under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI), which were made under sections 60 (now section 251 of the NHS Act 2006) and 64 of the Health and Social Care Act 2001. Data will only be extracted for those patients who have consented to the process. Provider – BioBank
COVID-19 vaccinations for housebound patients and care home residents	Purpose – Hastings & Rother Healthcare may securely share limited patient information with J Andersen Pharmacy, a third-party community pharmacy provider acting on our behalf, to support the delivery of COVID-19 vaccinations to eligible housebound patients and care home residents. J Andersen Pharmacy will use the information to: • contact eligible patients or their appropriate representative; • arrange a suitable date and time for a vaccination visit; • confirm vaccination eligibility and previous vaccination history; • administer the vaccination where appropriate; and • notify the Practice of the vaccination outcome, including where a vaccination has been declined, so that the patient's medical record can be updated. The information shared may include the patient's: • name; • date of birth and age; • NHS number; • home or care home address; and • telephone and mobile telephone numbers. Information will be transferred securely using NHSmail and a password-protected file. J Andersen Pharmacy will record

	vaccination information using the secure Cegedim Pharmacy Services Manager system. Patients remain free to accept or decline the vaccination. Consent to receive the vaccination is separate from the lawful basis used to process and share information to arrange and provide the service. Consent to vaccination will be confirmed and recorded by the vaccinating pharmacist before the vaccination is administered. Where there is reason to believe that a patient may be unable to make the vaccination decision themselves, the vaccinator will follow the Mental Capacity Act 2005. This will include making reasonable adjustments, assessing and recording the patient's capacity to make the specific decision and, where appropriate, making and documenting a best-interests decision. Any valid health and welfare Lasting Power of Attorney, court-appointed deputy or relevant advance decision will be considered, and the patient will be involved in the decision as far as reasonably possible. Legal Basis – 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 Practice. UK GDPR Article 9(2)(h): processing is necessary for the provision of health care or treatment or the management of health and care services. Data Controller – Hastings & Rother Healthcare remains the Data Controller for information shared from the GP medical record. Data Processor – J Andersen Pharmacy. System provider/Sub-processor – Cegedim Rx Ltd. Retention – The temporary patient list will be held by J Andersen Pharmacy for the duration of the vaccination programme and for no more than 30 days following completion of the programme to manage any immediate queries or complaints. It will then be securely deleted. Vaccination information added to the patient's clinical record will be retained in accordance with NHS records-management requirements.

General practice data for planning and research (GDPR)	**Purpose:** Patients personal confidential data will be extracted and shared with NHS Digital in order to support vital health and care planning and research. Further information can be found here Patients may opt out of having their information shared for Planning or Research by applying a National Data Opt Out or a Type 1 Opt Out. Details of how to Opt Out can be found on our Privacy Notice. For the National Data Opt Out patients are required to register their preference below. https://www.nhs.uk/your-nhs-data-matters/ For Type 1 Opt Out they can complete the form and return it to their registered practice for action by the 23rd June 2021. https://nhs-prod.global.ssl.fastly.net/binaries/content/assets/website-assets/data-and-information/data-collections/general-practice-data-for-planning-and-research/type-1-opt-out-form.docx **Legal Basis :** The legal basis for this activity can be found at this link : General Practice Data for Planning and Research: NHS Digital Transparency Notice – NHS Digital **Processor:** NHS Digital
General practice extraction service (GPES) , covid-19 planning and research data	Purpose : Personal confidential and Special Category data will be extracted at source from GP systems for the use of planning and research for the Covid-19 pandemic emergency period. Requests for data will be required from NHS Digital via their secure NHSX SPOC Covid-19 request process. Legal Basis : NHS Digital has been directed by the Secretary of State under section 254 of the 2012 Act under the COVID-19 Direction to establish and operate a system for the collection and analysis of the information specified for this service: GPES Data for Pandemic Planning and Research (COVID-19). A copy of the COVID-19 Direction is published here: https://digital.nhs.uk//about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/covid-19-public-health-directions-2020 Patients who have expressed an opt out preference via Type 1 objections with their GP surgery, not to have their data extracted

	for anything other than their direct care will not be party to this data extraction. Processor : NHS Digital
General data extraction service (GPES), cvdprevent audit	**Purpose :** NHS England has directed NHS Digital to collect and analyse data in connection with Cardiovascular Disease Prevention Audit (referred hereafter to as "CVDPREVENT Audit"). The NHS Long Term Plan identifies cardiovascular disease (CVD) as a clinical priority and the single biggest condition where lives can be saved by the NHS over the next 10 years. CVD causes a quarter of all deaths in the UK. This General Practice Extraction Service (GPES) data will be extracted as an initial full-year extract of data and thereafter as an extract on a quarterly basis. The first extract is scheduled to take place in the second half of 2020-21 financial year and will cover the previous financial year of 2019-20. **Legal Basis**: All GP Practices in England are legally required to share data with NHS Digital for this purpose under section 259(1)(a) and (5) of the 2012 Act **Processor**: NHS Digital
Medication/ Prescribing	**Purpose :** Prescriptions containing personal identifiable and health data will be shared with chemists/pharmacies, in order to provide patients with essential medication or treatment as their health needs dictate. This process is achieved either by face to face contact with the patient or electronically. Where patients have specified a nominated pharmacy they may wish their repeat or acute prescriptions to be ordered and sent directly to the pharmacy making a more efficient process. Arrangements can also be made with the pharmacy to deliver medication **Legal Basis :** Article 6(1)(e); "necessary… in the exercise of official authority vested in the controller' And Article 9(2)(h) as stated below Patients will be required to nominate a preferred pharmacy.

	Processor – Pharmacy of choice
GP Registrar & GP Trainee	**Purpose –** We are a GP training surgery. On occasion you may be asked if you are happy to be seen by one of our GP registrars. You may also be asked if you would be happy to have a consultation recorded for training purposes. These recordings will be shared and discussed with training GPs at the surgery, and also with moderators at the RCGP and HEE. **Legal Basis –** 6 1 (a) consent, patients will be asked if they wish to take part in training sessions. **9 2 (a) –** explicit consent will be required when making recordings of consultations Recordings remain the control of the GP practice and they will delete all recordings from the secure site once they are no longer required. **Processor** – RCGP, HEE, iConnect, Fourteen Fish
Learning disability mortality programme LEDER	**Purpose :** The Learning Disability Mortality Review (LeDeR) programme was commissioned to improve the standard and quality of care for people with a learning disability. **Legal Basis:** It has approval from the Secretary of State under section 251 of the NHS Act 2006 to process patient identifiable information without the patient's consent. **Processor :** Bristol University.
Technical solution, anticoagulation monitoring	**Purpose:** Personal confidential and special category data in the form of medical record, is extracted under contract for the purpose of pseudonymisation. This will allow no patient to be identified within the data set that is created. SCWCSU has been commissioned to provide a data processing service, no other processing will be undertaken under this contract.

	Legal Basis: Under GDPR the legitimate purpose for this activity is under contract to provide assistance. 6 1 (e) Public Task 9 2 (h) Health Care **Processor**: SCW CSU **Purpose:** Personal Confidential data is shared with LumiraDX in order to provide an anticoagulation clinic to patients who are on anticoagulation medication. This will only affect patients who are within this criteria. **Legal Basis**: The legal basis for this activity under UK GDPR is Article 6 1 (b) processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract. Article 6 (e) Public Task (Direct Care) and 9 2 (h) Health Data **Processor** : LumiraDX INRStar
Emotional Wellbeing Service and PHC SMI Facilitator Service	**Purpose** – Access to medical records is provided to social prescribers to undertake a full service to patients dependent on their social care needs. **Legal Basis** – (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. **Processor** – SPFT (Sussex Partnership Foundation Trust)
Mental Health Support Coordinators from Southdown	**Purpose** – the provision of an enhanced mental health service (consent required). **Legal Basis** - PCN lawful bases for processing are: Art 6(1)e) - public task/ official authority to provide direct care Art 9(2)h) - health and social careTo prevent function creep, the data processing contract specifies that data will only be processed for the designated purpose of providing mental health services. Any changes to this process would require a new Data Protection Impact Assessment (DPIA) to be conducted.

	Contractual Processor – Southdowns
PCN Podiatry Service	**Purpose:** The primary purpose of the PCN running a 'first contact' Podiatry service is to provide additional Podiatry resource to patients and to assist with alleviating pressure from GP Practices. It will allow us to ensure accurate diagnosis and treatment of foot and lower limb conditions and to educate patients on managing these conditions more effectively. The PCN Podiatry service will also enhance patient outcomes when working more effectively with external healthcare providers. The individuals will be patients within our PCN who have been referred into the service by their registered GP or other referring clinician. There will be a direct care relationship where patients will expect their data to be used for their Podiatry related care **Legal basis** – PCN lawful bases for processing are: Art 6(1)e) - public task/ official authority to provide direct care **Contractual Processor: PCN**
We work in partnership with Medical Universities and Colleges: Kings College London Brighton and Sussex Medical School University College London Hospital	**Purpose:** For the provision of patient care and related administrative purpose, in order to train medical students to become doctors or doctors intending to become general practitioners **Legal basis:** Art 6(1)e) - public task/ official authority to provide direct care , "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 Data Controller". **Processor:** Pebble Pad,

Enhanced Lung Care Screening Programme - Pilot	**Purpose:** To identify patients and invite them to take part in an Enhanced Lung Care Screening. The purpose of this screening is to identify and treat lung conditions to improve outcomes. **Legal Basis:** **Article 6(1)e** "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; **Article 9(2)h** "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services"; **Processor:** InHealth
GP Connect including local HTML viewers: Sussex Shared Care Record (Plexus)	**Who We Are** Your GP practice is the data controller of your GP medical record. This means we are legally responsible for how your information is used, shared, and protected. When other services (such as hospitals or social care teams) are involved in your care, they may also act as data controllers for the information they generate. However, we remain responsible for any access to your GP data, including access through shared systems like Plexus Shared Care Record. **What is GP Connect?** **GP Connect** is a national service that allows authorised health and social care workers (under role-based access control) from GP practices and a variety of care settings to share and access their patients' GP records for the purpose of direct patient care. **What is Plexus Shared Care Record?** Plexus Shared Care Record is the name of the Sussex Shared Care Record programme. It enables secure, read-only access to patient information by authorised health and care professionals across Sussex. This includes data viewing through GP Connect, which provides HTML views of GP records via platforms such as

	Plexus (AKA Sussex Shared Care Record), and other health and care provider systems. These other systems include those used by Ambulance Services and Digital Social Care Record Providers (such as Care Vision, Nourish, PCS, CareBeans etc.). **Sussex Organisations with Access via Plexus** These include: • University Hospital Sussex NHS Foundation Trust • East Sussex Healthcare NHS Trust (ESHT) • Queen Victoria Hospital • Sussex Community NHS Foundation Trust • Sussex Partnership NHS Foundation Trust • 111 Staff who access the system must be involved in your care and authorised via their organisation's access controls. **Restricted Views for Local Authorities and Care Homes** • Local Authorities (limited access for Social Workers) • Care Homes (limited, read-only access) Access for these organisations is intentionally limited and controlled. The available information and views are detailed on NHS England's site: GP Connect Access Record - NHS England Digital **How the Information is Used – Benefits and Risks** GP Connect data access supports: • Safer, more effective care by providing professionals access to current, relevant information • Fewer delays in care delivery • Fewer errors and reduced need to repeat your history More on benefits of GP Connect: https://transform.england.nhs.uk/key-tools-and-info/data-saves-lives/

	However, there is always a risk that without adequate governance, inappropriate access could occur. Strict access controls and audit logs are in place to monitor this. **Legal Basis for Sharing** We share information to support your direct care under: • **UK GDPR Article 6(1)(e)** – processing is necessary for the performance of a public task • **UK GDPR Article 9(2)(h)** – processing is necessary for the provision of health or social care This is supported by legislation such as the Health and Social Care Act 2012 and the Health and Care (Safety and Quality) Act 2015. **Your Data, Your Rights** You have the right to: • Be informed about how your data is used • Request access to your information • Correct inaccurate data • Object to sharing – if you do not want your GP data shared via Our Care Connected or GP Connect, you can opt out. Contact your practice for details. Please note: the national Type 1 Opt-Out does not apply to this form of direct care sharing. If patients do not wish their information to be shared using GP Connect, they can opt out by contacting their GP practice.
NHSMail and Office 365 (N365 Applications and SharePoint)	**Purpose**: NHSmail and Office 365 help NHS staff work more securely and efficiently which directly benefits our patients: • **Security**: Emails are encrypted keeping your sensitive information safe. • **Collaboration**: Staff can easily work together saving time and improving care.

	• **Reliability**: The system is supported 24/7 to avoid service disruptions. • **National Reach**: Staff can easily connect across different NHS organisations. • **Safety**: Advanced protection against viruses and spam keeps information secure. • **Flexibility**: Staff can communicate without disruption even if organisations change. These tools support the NHS's goal of improving digital care and collaboration. **Legal Basis**: **Article 6(1)e** - "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; **Article 9(2)h** - "processing is necessary for the purposes of preventive or occupational medicine"; **Processor**: Accenture **Sub-processor:** Microsoft

Reviews of and Changes to our Privacy Notice

We will keep our Privacy Notice under regular review. This notice was last reviewed in September 2024.

Lawful basis for processing:

The processing of personal data in the delivery of direct care and for providers' administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 and 9 conditions of the GDPR:

- Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and
- Article 9(2)(h) 'necessary for the purposes of preventative 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…"