THE MILL
MEDICAL PRACTICE

Fair Processing Notice (Privacy Notice)

Your Personal Information – what you need to know

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.

Please note CCTV is in place at the surgery for the Health and Safety of patients and staff. CCTV footage is kept for a period of 49 days.

Please note that telephone calls are recorded for the purpose of Quality Assurance. Call recordings are kept until we reach our maximum storage limit. Once it reaches 30GB, after this point previous recordings will be overwritten from the oldest call.

From time to time we may need to outsource some of the dictations made by the GP's within the surgery. This does not happen very often, and only when it is to provide a more efficient service to patients (e.g to cover staff holiday or sickness.) We use Lexacom. The data is transferred in encrypted format using either AES-256 or TLS encryption. The data has a retention period of 90 Days.

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

In order to deliver the best possible service, the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf, we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share the information other than in accordance with our instructions and that they operate securely.

Examples of functions that may be carried out by third parties include companies that provide;

- IT services and support, including our clinical systems,
- systems which manage patient facing services (e.g. our website)

- Data hosting service providers,
- Systems which facilitate appointment bookings, electronic prescription services,
- Document management services

Improvements in information technology are also 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.

Statutory disclosures

Sometimes we are duty bound by laws to disclose information to organisations such as the Care Quality Commission, the Driver and Vehicle Licencing Agency, the General Medical Council, Her Majesty's Revenue and Customs and Counter Fraud services. In these circumstances we will always try to inform you before we are required to disclose and we only disclose the minimum information that the law requires us to do so

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 or with consent.

Pseudonymised or anonymised data is generally used for research and planning so that you cannot be identified.

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.

Safeguarding of children or vulnerable adults

If we have significant concerns or hear about an individual child or vulnerable adult being at risk of harm, we may share relevant information with other organisations, such as local authorities and the Police, involved in ensuring their safety.

How long do we hold information for?

All records held by the Practice will be kept for the duration specified by national guidance from Records Management Code of Practice - NHS England Digital. 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 2021.

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 known 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.

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

Right of Access to your information (Subject Access Request)

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

- It may be deemed to risk causing harm to the patient or others
- The information within the record may relate to third parties who are entitled to their confidentiality, or who have not given their permission for the information to be shared.

Patients do not need to give a reason to see their data. And requests can be made verbally or in writing. Although we may ask them to complete a form in order that we can ensure that they have the correct information required.

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

Patients will need to provide proof of identity to receive this information. We will not share information relating to you with other individuals without your explicit instruction or without sight of a legal document.

Patients may also request to have online access to their data, they may do this via the NHS APP, or via the practice's system. Further information about the service can be found at the **privacy notices for the NHS App** managed by NHS England.

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, or if any of your other contacts details are incorrect including third party emergency contact details. 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.

We also use the NHS Account Messaging Service provided by NHS England 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 England.

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 registerat: https://ico.org.uk/esdwebpages/search

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 our Data Protection Officer via the surgery at: millmedicalpractice@nhs.net

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 have concerns or are unhappy about any of our services, please contact the Practice Managers Sue Bonner or Louise Bowers.

For independent advice about data protection, privacy and data-sharing issues, you can contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Phone: 0303 123 1113 Website: https://ico.org.uk/global/contact-us

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.

Activity	Rationale
Commissioning and contractual purposes Planning Quality and Performance	**Purpose –** Anonymous data is used by the Integrated Care Board (ICB) for planning, performance and commissioning purposes, as directed in the practices contract, to provide services as a public authority. **Legal Basis** – • 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' Patients may opt out of having their personal confidential data used for planning or research. Please contact your surgery to apply a Type 1 Opt out or logon to https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/ to apply a National Data Opt Out **Processor** – NHS Surrey & Sussex ICB
Summary Care Record Including additional information	**Purpose –**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** – • 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'

	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: https://digital.nhs.uk/services/summary-care-records-scr/scr-patient-consent-preference-form and returned to the practice. Please note that opting out of having your information shared with the Summary Care Record could result in a delay to care that may be required in an emergency. **Processor –** NHS England
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 standard NHS contract. 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 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 but this may affect the decision to provide individual funding. **Legal Basis** – • 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' **Data processor** – NHS Surrey & Sussex ICB
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 and to protect the safety of individuals. Consent is not required to share information for this purpose. **Legal Basis** – Direct Care under UK 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 **Data Processor** – Multi-agency Safeguarding Hub(MASH), Surrey-wide Safeguarding Team
Safeguarding Children	**Purpose –** We will share children's personal information where there is a need to assess and evaluate any safeguarding concerns and to protect the safety of children.

	Legal Basis – • 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' Consent may not be required to share this information. Data Processor – Surrey CC, Children's Single Point of Access. Surrey-wide Safeguarding Team
Surrey Child and Family Health Service - HCRG Care Group	**Purpose –** To deliver health care to patients, the sharing of relevant and appropriate clinical information between GP practices and the Surrey Children's services **Legal basis –** • 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' **Data processor** – HCRG Care Group
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 – • 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' **Processors** – As contracted by NHSE/ICB
Public Health Screening programmes (identifiable) Notifiable disease information (identifiable) Smoking cessation (anonymous) Sexual health (anonymous) Vaccination Programmes	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 to name a few. The law allows us to share your contact information, and certain aspects of information relating to the screening with Public Health England so that you can be appropriately invited to the relevant screening programme. More information can be found at: Population screening programmes - GOV.UK or speak to the practice. Patients may not opt out of having their personal information shared for Public Health reasons. Patients may opt out of being screened at the time of receiving an invitation. **Legal Basis** – • 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' **Data Processors** - Surrey County Council – Public Health England
Vaccination and immunisation uptakes	Aggregated patient extracts are shared with the UK Health Security Agency for the purposes of vaccination and immunisations uptake monitoring. For more information, see the UKHSA privacy notice: UKHSA privacy notice - GOV.UK **Processor -** UK Health Security Agency
Direct Care NHS Trusts Community Providers Pharmacies Enhanced care providers Nursing Homes Other Care Providers	**Purpose –** Personal information is shared with other secondary care trusts and providers in order to provide you with individual 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(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 **Processors** - Royal Surrey NHS Foundation Trust, Frimley Health Foundation Trust, Surrey and Borders Partnership NHS Trust and other providers as necessary for the delivery of individual direct care services.
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 their 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
Population Health Management	**Purpose –** Health and care services work together as 'Integrated Care Systems' (ICS) and are sharing data in order to: • Understand the health and care needs of the care system's population, including health inequalities • Provide support to where it will have the most impact • Identify early actions to keep people well, not only focusing on people in direct contact with services, but looking to join up care across different partners. **Type of Data –** Identifiable/Pseudonymised/Anonymised/Aggregate Data. NB only organisations that provide your care will see your identifiable data. **Legal Basis** – • 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 **Data Processors -** Optum, Cerner
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 data base	**Purpose –** Your medical record will be processed in order that a data base can be maintained, this is managed in a secure way and there are robust processes in place to ensure your medical record is kept accurate, and up to date. Your record will follow you as you change surgeries throughout your life. Closed records will be archived by NHS England **Legal Basis** – • 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'. **Processor** – EMIS and PCSE
Medical reports	**Purpose –** Your medical record may be shared in order that:

Subject Access Requests	Solicitors/persons acting on your behalf can conduct certain actions as instructed by you. Insurance companies seeking a medical reports where you have applied for services offered by then can have a copy to your medical history for a specific purpose. **Legal Basis** – • Article 6(1)(a) – consent for personal data; and • Article 9(2)(a) – explicit consent for special-category data. **Processor –** Solicitors and insurance organisations, IGPR
Medicines Management Team Medicines Optimisation	**Purpose** – Your medical record is shared with the medicines management team pharmacists, in order that your medication can be kept up to date and any necessary changes to medication can be implemented. **Legal Basis** – • 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' **Processor** NHS Surrey & Sussex ICB medicines management team
GP Federation	**Purpose –** Your medical record will be shared with Procare in order that they can provide direct care services to the patient population. This could be in the form of Minor injuries 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** – Procare Health Limited
PCN(Primary Care Network)	**Purpose –** Your medical record will be shared with the active PCN in order that they can provide direct care services to the patient population. **Legal Basis** – • 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' **Processor** – Binscombe Medical Practice, Cranleigh Medical Practice, Springfield Surgery, Wonersh Surgery

Smoking cessation	**Purpose –** personal information is shared in order for the smoking cessation service to be provided. Only those patients who wish to be party to this service will have their data shared **Legal Basis** – • 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' **Processor –** One You Surrey
Subject Access Requests Requestors	**Purpose –** Personal information will be shared with the person or their representative at their request **Legal Basis –** Contractual agreement with the patient – and consented **Processor –** Patients and or their representatives – e.g. family members, solicitors, insurance companies
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 –** Personal confidential information may be shared with the Police authority for certain purposes. The level of sharing and purpose for sharing may vary. Where there is a legal basis for this information to be shared consent will not always be required. The Police will require the correct documentation in order to make a request. This could be but not limited to, DS 2, Court order, s137, the prevention and detection of a crime. Or where the information is necessary to protect a person or community. **Legal Basis –** UK GDPR • Article 6(1)(c) – to comply with a legal obligation; and • Article 9(2)(j) – 'for reasons of substantial public interest' **Processor –** Police Constabulary
Coroners	**Purpose –** Personal health records or information relating to a deceased patient may be shared with the coroner**.** **Legal Basis –** UK GDPR: • Article 6(1)(c) – to comply with a legal obligation; and

	• Article 9(2)(h) – 'necessary for the purposes of preventative or occupational medicine'. **Processor –** The Coroner
Medical Examiner Service Royal Surrey NHS Foundation Trust	**Purpose**: Purpose: Medical records associated with deceased patients are outside scope of the UK GDPR. However, next of kin details are within the scope of the UK GDPR. We will share specified deceased patient records and next of kin details with the Medical Examiners within Royal Surrey NHS Foundation Trust. **Legal Basis**: Article 6(1)(c) – necessary under a legal obligation to which the controller is subject"; and 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**: Medical Examiners service – Royal Surrey NHS Foundation Trust
Non-commissioned, private healthcare providers (e.g. BUPA, Virgin Care, etc.)	**Purpose –** Personal information shared with private health care providers in order to deliver direct care to patients at the patient's request. Consent from the patient will be required to share data with Private Providers. **Legal Basis –** Articles 6(1)(a) and 9(2)(a) consent by the patient given under contract to the provider. **Provider** – As per patients choice
Messaging Service	**Purpose –** Personal identifiable information shared with the messaging service in order that messages including; appointment reminders; results; campaign messages related to specific patients health needs; and direct messages to patients, can be transferred to the patient in a safe way. **Legal Basis** – • 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' **Provider -** AccuRX, NHSAPP, Mjog, Rapid Health, NHS Mail

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** – • 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' Patients may be videoed or asked to provide photographs with consent. 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 identifiable pictures of children. **Processor -** AccuRX
MDT meetings	**Purpose** – For some long term conditions, the practice participates in meetings with staff from other agencies involved in providing care, to help plan the best way to provide care to patients with these conditions. Personal data will be shared with other agencies in order that mutual care packages can be decided. **Legal Basis** – • 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' **Processor –** Via MS Teams, shared with Royal Surrey NHS Foundation Trust clinicians, Procare District Nurses, clinicians directly involved in patients care e.g Phyllis Tuckwell
General Practice Extraction Service (GPES) At risk patients data CVDPREVENT Audit Physical Health Checks for people with Severe Mental Illness National Obesity Audit Covid-19 Planning and Research data	**Purpose –** GP practices are required to provide data extraction of their patients personal confidential information for various purposes to NHS England. The objective of this data collection is on an ongoing basis to identify patients registered at General Practices who fit within a certain criteria, in order to monitor and either provide direct care, or prevent serious harm to those patients. Below is a list of the purposes for the data extraction, by using the link you can find out the detail behind each data extraction and how your information will be used to inform this essential work: 1. At risk patients including severely clinically vulnerable 2. NHS England has directed NHS England to collect and analyse data in connection with Cardiovascular Disease Prevention Audit

	3. GPES Physical Health Checks for people with Severe Mental Illness (PHSMI) data collection. 4. National Obesity Audit - NHS Digital 5. Covid-19 Planning and Research data **Legal Basis -** All GP Practices in England are legally required to share data with NHS England for this purpose under section 259(1)(a) and (5) of the The Health and Social Care Act 2012 Further detailed legal basis can be found in each link. Any objections to this data collection should be made directly to NHS England. enquiries@nhsdigital.nhs.uk **Processor –** NHS England
Medication/Prescribing	**Purpose:** Prescriptions containing personal identifiable and health data will be shared with organisations who provide medicines management including chemists/pharmacies, in order to provide patients with essential medication regime management, medicines and or treatment as their health needs dictate. This process is achieved either by face to face contact with the patient or electronically. Pharmacists may be employed to review medication**,** Patients may be referred to pharmacists to assist with diagnosis and care for minor treatment, patients may 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 care and medication **Legal Basis** – • 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' **Processor** – Pharmacy of choice
GP Registrar - trainee	**Purpose –** We are a training surgery. Our clinical team are required to be exposed to on the job, clinical experience, as well as continual professional development. On occasion you may be asked if you are happy to be seen by one of our GP registrars, pharmacists or other clinical team to assist with their training as a clinical professional. 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 • 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' 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, HEEKSS, Fourteen Fish
Telephony	**Purpose –** The practice use an internet based telephony system that records telephone calls, for their own purpose and to assist with patient consultations. The telephone system has been commissioned to assist with the high volume and management of calls into the surgery, which in turn will enable a better service to patients. We record incoming and outgoing calls. Our phone system is set to automatically retain calls for 30 GB. After this point, the recordings are automatically deleted. The 30GB retention period enables us to download and retain exact and unaltered copies of calls where required for medico-legal purposes. **Legal Basis –** While there is a robust contract in place with the processor, the surgery has undertaken this service to assist with the direct care of patients in a more efficient way. • 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' **Provider –** Babblevoice
Learning Disability Mortality Programme LeDer	**Purpose:** The Learning Disability Mortality Review (LeDeR) programme was commissioned by NHS England to investigate the death of patients with learning difficulties and Autism to assist with processes to improve the standard and quality of care for people living with a learning disability and Autism. Records of deceased patients who meet with this criteria will be shared with NHS England. **Legal Basis:** It has approval from the Secretary of State under section 251 of the NHS Act 2006 to process patient identifiable information who fit within a certain criteria.

	Processor : ICB, NHS England
Shared Care Record	**Purpose:** In order for the practice to have access to a shared record, the Integrated Care Service has commissioned a number of systems including GP connect, which is managed by NHS England, to enable a shared care record, which will assist in patient information to be used for a number of care related services. These may include Population Health Management, Direct Care, and analytics to assist with planning services for the use of the local health population. Where data is used for secondary uses no personal identifiable data will be used. Where personal confidential data is used for research explicit consent will be required. **Legal Basis** – • 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' **Processor:** NHS England
Anticoagulation Monitoring	**Purpose:** Personal Confidential data is shared with LumiraDX and INRStar 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** – • 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' **Processor** : LumiraDX INRStar
Local shared care record Graphnet Portal, Surrey Care Record	**Purpose:** Health and Social care services are developing shared systems to share data efficiently and quickly. It is important for anyone treating you to be able to access your shared record so that they have all the information they need to care for you. This will be during your routine appointments and in urgent situations such as going to A&E, calling 111 or going to an Out of hours appointment. It is also quicker for staff to access a shared record than to try to contact other staff by phone or email.

	Only authorised staff can access the systems and the information they see is carefully checked so that it relates to their job. Systems do not share all your data, just data which services have agreed is necessary to include. **Legal Basis** – • 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' **Processor:** Graphnet, Surrey & Sussex ICB
Technical Solution	**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
General Practice Data for Planning and Research(GPDPR)	**Purpose:** To support a wide variety of research and analysis to help run and improve health and care services. **Legal Basis**: The Health and Social Care Act 2012 (2012 Act) covers the sharing and collection of health and care data. **Processor:** NHS digital This practice is supporting vital health and care planning and research by sharing your data with NHS Digital. For more information about this see the GP Practice Privacy Notice for General Practice Data for Planning and Research.
Third party	In order to deliver the best possible service, the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf, we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share the information other than in accordance with our instructions and that they operate securely. Examples of functions that may be carried out by third parties include companies that provide; • IT services and support, including our clinical systems,

	• systems which manage patient facing services (e.g. our website) • Data hosting service providers, • Systems which facilitate appointment bookings, electronic prescription services, • Document management service
GP connect	**Purpose:** We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patients care, leading to improvements in both care and outcomes. GP Connect is not used for any purpose other than direct care. Authorised Clinicians such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect. The NHS 111 service (and other services determined locally e.g. Other GP practices in a Primary Care Network) will be able to book appointments for patients at GP practices and other local services. **Legal basis for sharing this data:** In order for your Personal Data to be shared or processed, an appropriate "legal basis" needs to be in place and recorded. The legal bases for direct care via GP Connect is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider: • for the processing of personal data: Article 6.1 (e) of the UK GDPR: "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". • for the processing of "Special Category Data" (which includes your medical information): Article 9.2 (h) of the UK GDPR: "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". Your rights Because the legal bases used for your care using GP Connect are the same as used in other direct care situations, the legal rights you

	have over this data under UK GDPR will also be the same- these are listed elsewhere in our privacy notice. Find out more about GP connect here: https://digital.nhs.uk/services/gp-connect or read the Transparency notice here: https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation/transparency-notice
Heidi Health	Purpose : We use an AI-powered medical scribe, Heidi Health, to aid with documenting consultations, transcribing patient visits and letter dictations. This tool allows us to focus more on the consultation rather than on typing and administrative tasks. • Enhanced Focus on Patient Care - By automating the documentation process, Heidi Health allows us to spend more time interacting with you, improving the quality of care and communication during consultations. • Efficiency and Accuracy - The AI scribe ensures that all details of your visit are accurately recorded, reducing the risk of errors and omissions in your medical records. • Streamlined Workflow - Heidi Health helps in managing various administrative tasks such as generating patient summaries and creating letters, making our workflow more efficient. • Data Security and Privacy - Heidi Health adheres to stringent UK compliance frameworks, including the Data Protection Act, Cyber Essentials, GDPR and NHS standards such as DCB0129, DTAC and DSPT. This ensures that your personal information is handled securely and confidentially. More information can be found at: https://trust.heidihealth.com https://www.heidihealth.com/uk/legal/ukgdpr-compliance-policy Local Data Hosting - All data is hosted within the UK, enhancing security and compliance with local data protection regulations. Temporary Data Storage - Audio recordings used for generating notes are not stored permanently. They are processed and then deleted, ensuring data remains private and secure. **Processor:** Heidi Health
Healthtech1	Healthtech1 is a web-based system that integrates with the electronic health record to automation new patient registrations. It takes the information from the patient submitted online NHS England, PRF1 form and compares that information with the NHS Spine database. Mismatched data is flagged to the practice for checking, and correctly matched data is automatically processed into the EHR. The privacy policy of Healthtech1 can be found here. **Legal basis for sharing this data.**

	In order for your Personal Data to be shared or processed, an appropriate "legal basis" needs to be in place and recorded. The legal basis for direct care via Healthtech1 is the same as the legal basis for the care you receive from your own GP, or another healthcare provider. · For the processing of personal data: Article 6.1 (e) of the UK GDPR: "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". · For the processing of "Special Category Data" (which includes your medical information): Article 9.2 (h) of the UK GDPR: "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**: Healthtech-1 Ltd.
OpenSAFELY	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 a type 1 opt out with their GP. You can find additional information about OpenSAFELY at https://www.opensafely.org/ **Processor** – NHS England
ICT systems	We utilise the services of ICT system providers to support the delivery of activities and act as data processors.
RapidHealth	Purpose: We use a Smart Triage and Smart Booking system, Rapid Health, to aid with triaging and prioritising patient needs within the appointment booking system. We also use the system to send booking links to patients for pre-approved appointments. • Data Security and Privacy - Rapid Health has completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8KG49), and Cyber Essentials certification. Rapid Health has successfully completed NHS Digital Technology Access Criteria assurance (under NHS ODS code 8KG49). Rapid Health is fully compliant with DCB0129, which is for manufacturers of health IT software, and has a

	UKCA Class 1 medical device registered with the MHRA. Rapid Health systems are independently penetration tested by an accredited CREST/CHECK supplier to CREST/CHECK standards at least once a year. Rapid Health is GDPR compliant. • Personal Information Storage - Rapid Health stores the data on Amazon Web Services (AWS) servers in England. All data sent is encrypted when in transit (when it is sent) and at rest (when it is stored). Patient data is managed as described in the NHS Records Management Code of Practice and stored on the practice system. Rapid Health keeps a copy of requests for a year, for technical support purposes. They are deleted after a year. • Personal Data Access - Rapid Health must be able to access the information to meet its legal responsibilities as a data processor, for example to help the data controller (the practice) in providing subject access and allowing data subjects to exercise all their other rights under GDPR, and to provide technical support. Only highly qualified technical staff with permission can access the data when the data controller asks for this, or if there is a technical problem. Strong controls are in place and a full audit trail kept.
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.
iRhythm – Zio Service	**Purpose** : iRhythm provides the Zio service, which includes long-term heart monitoring and evaluation. Your doctor will, with your consent, start the Zio service by attaching an adhesive monitoring

	device to your chest. This device will collect your heart rhythm data. Your doctor will collect identification information such as your name, address and date of birth to safely identify your resulting heart rhythm report, and register it on iRhythm's physician portal. Your heart rhythm data will be sent to iRhythm when you return the Zio patch by post. iRhythm receives and processes your personal data in confidence to help create a report of the findings. Only iRhythm, your doctor and hospital will have access to this report for the purpose of supporting your direct care. iRhythm may also replace your direct identifying information with a reference number and study your heart rhythm data for two reasons: (i) reporting to your doctor and (ii) improvement of iRhythm services. **Use of AI** iRhythm uses AI to help eliminate the risks of error associated with a purely human review of heart rhythm data. Diagnostic systems do not use solely automated decision making but support rather than replace, clinician review by drawing upon derived understanding from analysing and comparing thousands of different heart rhythm patterns. This learning helps iRyhthm software to recognise and flag anomalies for closer inspection by cardiac physiologists, thereby enabling more efficient heart rhythm analysis for faster, more reliable diagnostic outcomes. **Lawful basis for processing personal data:** - Legitimate interest in patient healthcare and in supporting clinical treatment decisions – Art 6(1)(f) - Complying with legal obligations to which we are subject – Art 6(1)(c) - Necessary in any emergency situation in order to protect patient's vital interests (or the interests of another person) – Art 6(1)(d) **Lawful basis for processing special "sensitive" category data:** - Providing diagnostic services by supporting medical diagnosis for the purpose of healthcare treatment (processing is necessary for the purposes of medical diagnosis and the provision of health or social care or treatment – Art 9(2)(h)) - Public interest in the area of public health necessary for maintaining standards relevant to healthcare and medicinal products – Art 9(2)(i) - Research and statistical purposes in the public interest – Art 9(2)(j)

	Privacy Notice – information to individuals Each Zio Device comes with a hardcopy Patient Instruction and Button Press Log Booklet. The Booklet contains a Privacy Notice which provides information about the data being collected, the use of the information, and how patients can exercise their privacy rights by contacting iRhythm. iRhythm's patient notice can also be located here: http://www.irhythmtech.co.uk/patient-notice. There is no new data being gathered, and the information being processed is being used for the same purpose – the provision of health care. Processor: iRhythm
MEDLINK	**MedLink** We use **MedLink**, a secure digital healthcare platform provided by **MedLink Solutions Ltd**, to support the delivery of your direct care. MedLink may be used for a range of services, including: • Online health questionnaires and reviews • Long-term condition management • Medication monitoring • Collection of home readings and test results • Appointment booking and invitations • Patient communications and healthcare reminders • Other services that support your care When you use MedLink, information you provide is made available to our healthcare team and will be reviewed as part of your care. Where appropriate, information submitted through MedLink will become part of your healthcare record. **The Mill Medical Practice** is the **Data Controller** for your personal information and remains responsible for deciding how your personal information is used for your healthcare. **MedLink Solutions Ltd** acts as our **Data Processor**, processing personal information on our behalf in accordance with UK data protection legislation, NHS information governance requirements and our contractual agreement. Further information about how MedLink processes personal information, including details of security measures, approved sub-processors and your privacy rights, is available in the **MedLink Privacy Notice**: **MedlinkPrivacy Policy - MedLink**

Docman AI – One Advanced	We are looking to trial GP Workflow Assistant (Docman AI) which is an Artificial Intelligence-powered assistant within GP Document Workflow (Docman10X), designed to help GP surgeries review and manage their documents more efficiently. It enhances the process of summarising, reviewing, actioning and coding of clinical documents, reducing the time and effort required to complete manual administrative tasks. No data is stored in the AI product. Records are passed to Docman and the Practice PAS and these records are kept in line with the NHS Records Management code of practice. The GP Workflow Assist makes suggestion to the clinician around codes to be used; only approved users ensure the suggestions are correct before loading into the Docman. **Legal basis for sharing this data.** The lawful basis of healthcare staff using GP Workflow Assist for communicating with patients is: 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…' 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems The supplier OneAdvanced has a valid DSPT and Cyber Essentials Plus certification. The product has a RBAC which is integrated with the main Docman 10 Product. Processor – Docman
Accurx Scribe	Purpose : We use an AI-powered medical scribe, Accurx Scribe, to aid with documenting consultations, transcribing patient visits and letter dictations. This tool allows us to focus more on the consultation rather than on typing and administrative tasks. The lawful basis of healthcare staff using Accurx Scribe for communicating with patients is: 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'. 9(2)(h) '…medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems. Patients can object to the use of Accurx Scribe via their clinician. If they object, the clinician will document the consultation manually. This is consistent with the use of implied consent for direct care. **Processor-** Accurx

Electronic reporting solution – Managed Service	**Purpose**: The iGPR Electronic Reporting Solution provides GP Practices a solution to manage Subject Access Requests (SARs) under UK GDPR *and other requests for information* that are received from patients and third parties. The solution integrates directly with the practice clinical system. iGPR acts as a data Processor and securely reviews, prepares and supplies copies of medical records or reports when we as your GP practice are either legally required or when you have given your consent. **Legal Basis**: Under GDPR the surgery has used its legal basis of Article 6 1 (a) Consent Article 6 1 (e) Public Task - it is necessary for the performance of a task carried out in the public interest or under official authority vested in the controller Article 9 2 (a) health data - the data subject has given explicit consent 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 of Management of Health or Social Care Systems and Services on the basis of union or member state law or pursuant to contract with a health professional and subject to conditions and safeguards **Processor**: iGPR Technologies Ltd

Reviews of and Changes to our Privacy Notice

We will keep our Privacy Notice under regular review.

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..."

Review date:	Edited by:	Changes made:	Comments:
01.06.2026	SB	Added Accurx Scribe	

02.06.2026	SB	Added Vaccination and immunisation uptakes	
09.06.2026	SB	Added iGPR	
09.07.2026	CF	Updates to Medlink	
14.10.2026	SB	Updating links Updates to processors throughout GPES merged into one category Removal of research activity Removal of Minuteful Kidney Removal of Social Prescriber Removal of Covid Vaccination within GP federation INRStar added to purpose within Anticoagulation Monitoring	
19.11.26	CF	Added iRhythm and Zio Services	