Privacy Statement

How we use your information to provide you with healthcare

This Privacy Statement explains what Personal & Confidential Data (PCD) Salus Medical Services Limited (Salus) holds about you, why we hold it and how it is used.

Salus healthcare professionals who provide you with medical care maintain records about your health and about any treatment or care you have or have received previously. These records help to provide you with the best possible healthcare.

The information we hold is stored on secure NHS-approved computer systems and may include:

- Details about you, e.g. your address, carer, legal representative, emergency contact details.
- We may also record:
  a) Any contact Salus has had with you
  b) Notes and reports about your health
  c) Details about your treatment, medication and care
  d) Relevant information from other health professionals
  e) Information from relatives or those who care for you
- Information held about you may be used to help protect the health of the public and to help us manage NHS services. Information may be used within Salus for clinical audit to monitor the quality of the service provided.
- Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified.
- Our website gives you the opportunity to ask questions, send feedback or make a Subject Access Request. Any contact information you provide will only be used for the stated purpose.

How we ensure your records are held confidentially

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- General Data Protection Regulations 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality
- Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an organisation providing NHS services has a legal obligation to keep information about you confidential. Salus has deployed technical security measures to keep your information secure when being transferred electronically, including ensuring all security software and encryption is up to date to help prevent the risk of a cyber attack. All Salus staff have terms in their employment contract reinforcing that patient records must only ever be accessed for a legitimate purpose.

We will only ever use or pass on information about you in limited circumstances, such as:

- If others involved in your care have a genuine and lawful need for it
- You have provided your explicit consent for us to do so
- There are exceptional circumstances (e.g. life or death situations),
- Where the law requires information to be passed on
- In accordance with the information sharing principles set out in Dame Fiona Caldicott's information sharing review (Information: To share or not to share) which states that the duty to share information can sometimes be as important as the duty to protect patient confidentiality.

This means that health and social care professionals have the confidence to share information in the best interests of patients within the framework set out by the Caldicott principles. Salus has policies designed to help them do so.

It is your responsibility to tell us about any changes – please contact us at enquiries@salusmedical.co.uk.

It is important that you tell us, or your GP Practice, if any of your details such as your telephone number, name or address have changed or if any of your details such as date of birth is incorrect in order for this to be amended. You have a responsibility to inform us of any changes so your record is accurate and up to date.

You have the right to object to our sharing your data in some circumstances, but we have an overriding responsibility to do what is in your best interests. Please see below.

Other important information about how your information is used to provide you with healthcare and improve the NHS:

Identifying patients who might be at risk of certain diseases

Your medical records may be searched by a computer program so that we can identify patients who might be at high risk from certain conditions such as heart disease or diabetes. This means we can offer patients additional care or support as early as possible.

This process may also involve linking information from your GP record with information from other health or social care services you have used. Information which identifies you will only be seen by ourselves, your GP practice and by limited individuals at our Data Processor (NHS South, Central and West Commissioning Support Unit). For more information please contact us, see p2.

Safeguarding

Sometimes we need to share information so that other people, including healthcare staff, children or others with safeguarding needs, are protected from risk of harm. These circumstances are rare, but we do not need your consent or agreement to do this. Please see our local policies for more information, these are available from our admin office.

Medlink

We may offer registered patients the option to conduct a secure online review via a system called Medlink. If you agree to this, your data will be made available in Medlink in order to conduct the review and on completion it will attach a review summary to your permanent medical record. If appropriate (e.g. completing a vaccine consent form), you can request a copy of the document be sent to your personal email – the email address will not be used for any other purpose. Any PCD remaining on the system is anonymised and then deleted after 1 month.

AccuRx

AccuRx handles most of the text/SMS messages you receive from Salus or your GP. AccuRx does not store any PCD but it does process your information when sending messages. After transmission AccuRx stores the text in our electronic record system. In some cases you may be invited to complete an online form called a Florey and again this is processed but not stored by AccuRx. A copy of any completed Florey is held only in your medical record.

CCTV

Patients and staff attending Mayfield Medical Practice or the Farnborough PCN's Southwood Hub may be picked up on routine CCTV, installed for safety and to prevent or detect crime. It may be reviewed for staff training, and only shared beyond the practice if there is a crime involved. Recordings are kept in secure local storage accessible only to relevant Salus personnel and unless exceptionally required, deleted after 31 days. Footage that contains identifiable images will never be released to any person or body other than the police.

Integrated Care

If you or someone you care for has complex needs you may be referred to our Integrated Care Team (ICT) which brings together health and social care professionals from a range of local providers to assess your needs, create a care package, and monitor how we provide your care. The ICT includes Salus staff and representatives from local GPs, hospital, community nurses, community therapists, mental health, social services, social prescribers, Phyllis Tuckwell Hospice, Red Cross etc. Data relevant to your current and ongoing care needs will be shared as necessary and appropriate with the listed parties.

Our ICT also works with Consultants from Frimley Health Foundation Trust and local GP Practices to try to identify patients who may benefit from early intervention before their condition deteriorates. This is known as Proactive Care. If you or someone you care for is offered support under this scheme your records will be held and managed by our ICT.

A regional information sharing agreement is in place to ensure that all parties attending ICT meetings and AIM reviews are fully aware of their data security obligation to protect your PCD and have systems in place that satisfy the NHS data security standards. This document also covers the Community Single Point of Access described below.

Community Single Point of Access (CSPA)

Salus provides the CSPA for North East Hampshire and Farnham, meaning that if any medical professional makes a referral to a community-based service that is not accessible via the NHS Electronic Referral Service, the details will be processed and maintained by our CSPA hub. This simplifies the referral process for an increasingly diverse range of community-based services.

National Audits

We contribute to national clinical audits so that healthcare can be checked and reviewed. Information from medical records can help doctors and other healthcare workers measure and check the quality of care which is provided to you. The results of the checks or audits can show where services are doing well and where they need to improve.

The results of the checks or audits are used to recommend improvements to patient care. Data are sent to NHS Digital, a national body with legal responsibilities to collect data.

The data will include information about you, such as your NHS Number and date of birth and information about your health which is recorded in coded form, for example the code for diabetes or high blood pressure.

We will only share your information for national clinical audits or checking purposes when the law allows. For more information about national clinical audits see the Healthcare Quality Improvements Partnership website:

https://www.hqip.org.uk/ or phone 020 7997 7370.

You have the right to object to your identifiable information being shared for national clinical audits. Please contact us if you wish to object, see p2.

National Data Opt-Out (NDOO)

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 use a patient's confidential patient information for purposes beyond their individual care, for

Planning or Research. 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.

Public Health

We are required to share information with Public Health England if we become aware that you, a member of your family or people you have been in contact with are suffering from certain conditions known as Notifiable Diseases - often diseases that are rare in the UK such as Anthrax, Malaria or Leprosy but also Food Poisoning, Measles and Scarlet Fever. The law requires us to share your information to prevent the spread of these conditions and organisms that cause them.

Additionally, 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

Pinnacle/Covid-19 Vaccinations

Staff employed by Salus on behalf of Local GPs manage and operate Covid-19 vaccination centres at Southwood in Farnborough and Princes Hall in Aldershot. Staff working at these locations have access to your PCD stored in an NHS National System called Pinnacle which records your Covid-19 vaccination details and feeds information to the NHS App and to your GP Practice.

Salus also employs a small number of staff who run a service called Covid Oximetry at Home. This service is provided with information about newly diagnosed Covid-19 patients via your GP and we may contact you to offer support. Your PCD is held electronically for no more than 28 days from the date of your diagnosis.

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.

Patient Record Data Base - EMIS

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.

Surgery Connect

The practice uses an internet-based telephony system that records telephone calls, patients will have the right to decline recordings of calls as is their individual right. The calls will be held on the external server for a duration of 3 years unless requested for them to be removed sooner. 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.

Rapid Health

Rapid Health handles our triaging to provide you an instant medical assessment and secure an appointment or same-day response. Rapid Health stores the data on Amazon Web Services (AWS) servers in England. All data is sent 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 400 days, for technical support purposes. They are deleted after 400 days.

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 subject 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.

General Data Protection Regulations (GDPR) requires to provide you with the following information:

Data Controller	Salus Medical Services Limited Aldershot Centre for Health Hospital Hill ALDERSHOT GU11 1AY
Data Protection Officer	DPO: Lucy HUNT Email: enquiries@salusmedical.co.uk
Purpose of the processing	• To give direct health or social care to individual patients. For example, when a patient agrees to a direct care referral, such as to a hospital, relevant patient information will be shared with other health/care staff to enable them to appropriately advise, investigate, treat and/or care. • For checks and reviews of quality of care (audits and clinical governance.)
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..."*

	As noted above, there are several instances where your data might be processed because there is a legal requirement to do so. In such situations, our lawful basis would fall under: ***Article 6(1)(c)*** *'necessary for compliance with a legal obligation to which the controller is subject'* We will also recognise your rights established under UK case law collectively known as the "Common Law Duty of Confidentiality"
Recipient or categories of recipients of the processed data	The data will be shared with: • healthcare professionals and staff in this organisation • local hospitals • out of hours services • members of the Integrated Care Team • diagnostic and treatment centres or other organisations involved in the provision of direct care to individual patients • organisations providing National Screening Programmes or NHS audits We also share data with NHS South, Central and West Commissioning Support Unit who extract data from our systems and combine it with information from other sources such as local hospitals to undertake 'risk stratification', a process intended to help us identify patients most likely to need additional support and plan for that eventuality.
Rights to object	• You have the right to object to some or all the information being processed under Article 21. Please contact the Data Controller. You should be aware that this is a right to raise an objection; that is not the same as having an absolute right to have your wishes granted in every circumstance. • You are not able to object to your name, address and other demographic information being sent to NHS Digital. This is necessary if you wish to be registered to receive NHS care. • You are not able to object when information is legitimately shared for safeguarding reasons. In appropriate circumstances it is a legal and professional requirement to share information for safeguarding reasons. This is to protect people from harm. • You cannot object to us sharing data with the Care Quality Commission if they need it for their regulatory function.
Right to access and correct	• You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our 'Data Subject Access Request Form' on the website. • We are not aware of any circumstances in which you will have the right to delete correct information from your medical record; although if you believe there is no lawful purpose for which we hold the information please contact us, see p2.

Retention period	Salus medical records will be kept in line with the law and national guidance. Information on how long records are kept can be found in the: Records Management Code of Practice or speak to the DPO, see p6.
Right to complain	If you are happy for your data to be extracted and used for the purposes described in this Privacy Notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact Salus. In the first instance please contact the Data Controller via: FAO HR enquiries@salusmedical.co.uk You have the right to complain to the Information Commissioner's Office. If you wish to complain follow this link: https://ico.org.uk/global/contact-us/ or call the helpline 0303 123 1113
Data we get from other organisations	We receive information about your health from other organisations who are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what happens. This means your medical record is kept up-to date when you receive care from other parts of the health service.