



Fair Processing Notice (Privacy Notice)

Your Personal Information – what you need to know

Who we are and what we do

Surrey Heath Community Providers Ltd (SHCP) is responsible for securing some of the NHS services, in primary medical care (GP) services. These include the locally commissioned services and the integrated access (extended access service). We also have a performance monitoring role for these services, which includes ensuring that the highest quality of healthcare is provided and responding to any concerns from our patients on services offered. For further information please refer to the 'services' page on our Website:

<http://www.surreyheathcommunityproviders.co.uk/>

Our Commitment to Data Privacy and Confidentiality Issues

We 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.

Using your information

We need to use information about our patients and population to enable us to provide and support the direct care of individuals and to ensure we commission services which meet their needs.

In undertaking our role SHCP holds some information about you and this document outlines how that information is used, who we may share that information with, how we keep it secure (confidential) and what your rights are in relation to this. Within the health sector, we follow the common law duty of confidence, which means that where identifiable information about you has been given in confidence, it should be treated as confidential and only shared for the purpose of providing direct healthcare.

SHCP has a senior member of staff responsible for protecting the confidentiality of patient information. This person is called the Caldicott Guardian.



The details of our Caldicott Guardian are as follows:

Dr Sarah Stradling – Clinical Director
Tel: 07375646711
Email: shccg.enquiries.shcp@nhs.net

They are supported by another senior member of staff who is responsible for information risk and information security, this person is called the Senior Information Risk Owner (SIRO).

The contact details of our SIRO are as follows:

Ian Friend – Finance Director
Email: shccg.enquiries.shcp@nhs.net
Tel: 07375646711

The above two roles are also supported by our Data Protection Officer (DPO). The DPO is responsible for monitoring compliance with Data Protection legislations (GDPR & DPA 2018), Information Governance (IG) policies, providing advice and guidance, raising awareness, training and audits. The DPO acts as a contact point for the ICO, employees and the public. They co-operate with the ICO and will consult on any other matter relevant to Data Protection. The contact details of our DPO are as follows:

Tel: 07375646711
Email: shccg.enquiries.shcp@nhs.net

Surrey Heath Community Providers Ltd is a Data Controller and is registered with the Information Commissioner's Office (ICO) to collect data for a variety of purposes. Our registration number is **ZA464533** and a copy of the registration is available through the [ICO website](#).

What kind of information do we use?

As a commissioned service provider we hold or have access to your medical records and we hold personal information about you,

We use the following types of information/data:

- 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.

What do we use your Personal and Special categories of Personal Data for?

SHCP 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 on secure, NHS-approved systems and part of your GP Practice records. This may include:

- Details about you, such as your address, carer, legal representative, emergency contact details.
- We also record:
 - Any contact SCHP has had with you
 - Notes and reports about your health
 - Details about your treatment, medication and care
 - Relevant information from other health professionals
 - 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 SHCP 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.

What do we use non-identifiable data for?

We use pseudonymised, anonymised and aggregated data to plan health care services and help support Clinical Commissioning Groups for commissioned services. Specifically we use it to:

- check the quality and efficiency of the health services we provide/commission
- prepare performance reports on the services we provide/commission
- review the care being provided to make sure it is of the highest standard
- Evaluate the services we provide/commission or have been commissioned on our behalf
- To support the regional and national initiatives through the Integrated Care Systems (ICS)



Do we share your information with other organisations?

We commission NHS funded health services for you from a number of organisations, both within and outside the NHS (see Appendix A for details). We may also share anonymised statistical information for the purpose of improving local services, for example understanding how our populations health and how the services provided compare with similar services in other geographical areas e.g. to share good practice. We do not share information outside of the European Economic Area (EEA)

We would not share information that identifies you unless we have a fair and lawful basis such as:

- It is for Direct Care
- You have given us permission;
- We need to act to protect children and vulnerable adults;
- When a formal court order has been served upon us;
- When we are lawfully required to report certain information to the appropriate authorities e.g. to prevent fraud or a serious crime;
- Emergency Planning reasons such as for protecting the health and safety of others;
- When permission is given by the Secretary of State or the Health Research Authority on the advice of the Confidentiality Advisory Group to process confidential information without the explicit consent of individuals

How we process information

Data may be anonymised and linked with other data so that it can be used to improve health care and development and monitor NHS performance. Where data is used for these statistical purposes, stringent measures are taken to ensure individual patients cannot be identified.

We may also contract with other organisations to process data, some of which could identify a person. These organisations are known as Data Processors. We ensure external data processors that support us are legally and contractually bound to operate and are required to prove that robust security arrangements are in place.

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

What safeguards are in place to ensure data that identifies me is secure?

The [NHS Digital Code of Practice on Confidential Information](#) applies to all of our staff and anyone acting on behalf of SHCP. Each are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared. Each are expected to make sure information is kept confidential and undertake annual training on how to do this. This is monitored by SHCP and can be enforced through disciplinary procedures.

We also ensure the information we hold is kept in secure locations, restrict access to information to authorised personnel only, protect personal and confidential information held on equipment such as laptops with encryption (which codes data so that unauthorised users cannot see or make sense of it).



How long do we hold information for?

All records held by SHCP 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 sensitive 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.

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’. For further information please visit: [The NHS Constitution](#)

Information not directly collected by SHCP but collected by organisations that provide NHS services.
These are known as Type 1 and national data opt-outs and are described below:

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](#)

Gaining access to the data we hold about you

The SHCP does not directly provide health care services. If you wish to have sight of, or obtain copies of your own personal health care records you will need to apply to your **GP Practice, the hospital or NHS Organisation** which provided your health care.

If SHCP are holding information from which you can be identified, you have the right to:

- View this or request copies of the records by making a Right of Access request under the General Data Protection Regulation.
- request information is corrected/rectified
- have the information updated where it is no longer accurate



- where applicable, request information is erased
- where applicable, request for your data to be made portable
- where applicable, ask us to stop processing information about you where we are not required to do so by law

Everybody has the right to see, or have a copy, of data we hold that can identify you, with some exceptions. You do not need to give a reason to see your data. If you want to access your data you must make the request in writing. Under special circumstances, some information may be withheld.

For further information on how to make a request please visit our policies and procedures page on our website – <http://www.surreyheathcommunityproviders.co.uk/>

Automated Decision Making

SHCP will not make decisions based solely on automated processing

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 information that the CCG 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 ‘Gaining access to the data we hold about you’.

Your request must be in writing and can be either posted or emailed to;

By Email: shccg.enquiries.shcp@nhs.net

By Post: Freedom of Information
Surrey heath Community Providers Ltd
c/o Bartlett Group Practice
1 Beach road
Frimley Green
Camberley
Surrey
GU16 6QQ

Information Commissioners Office

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

By post: Information Commissioner’s Office
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

By telephone: 0303 123 1113 (local rate) or 01625 545 745



By email: casework@ico.org.uk or [Visit the ICO website](#).

Complaints or questions

We try to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring concerns to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. You can contact us by:

By telephone: 01252 335 054

By email: shccg.enquiries.shcp@nhs.net

By Post: Comments & Complaints Team
Surrey heath Community Providers Ltd
c/o Bartlett Group Practice
1 Beach road
Frimley Green
Camberley
Surrey
GU16 6QQ

Links to other websites

This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

Changes to this privacy notice

We keep our privacy notice under regular review. This Fair Processing Notice was last updated in January 2019.

Further information

Further information about the way in which the NHS uses personal confidential data and your rights in that respect can be found in:

The NHS Care Record Guarantee: This guarantee is a commitment that NHS organisations and those providing care on behalf of the NHS will use records about you in ways that respect your rights and promote your health and wellbeing.

<http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf>

The NHS Constitution: The Constitution establishes the principles and values of the NHS in England. It sets out rights to which patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with responsibilities, which the public, patients and staff owe to one another to ensure that the NHS operates fairly and effectively

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

To share or not to share? Information Governance Review: This was an independent review of information about service users shared across the health and care system led by Dame Fiona Caldicott and was conducted in 2012.



<https://www.gov.uk/government/publications/the-information-governance-review>

NHS Commissioning Board – Better Data, Informed Commissioning, Driving Improved Outcomes: Clinical Data Sets: Provides further information about the data flowing within the NHS to support commissioning.

<http://www.england.nhs.uk/wp-content/uploads/2012/12/clinical-datasets.pdf>

NHS Digital – Guide to Confidentiality: NHS Digital are the trusted national provider of high-quality information, data and IT systems for health and social care and are responsible for collecting data from across the health and social care system.

<http://digital.nhs.uk/patientconf>

Information Commissioner’s Office (ICO): The ICO is the Regulator for GDPR and offer independent advice and guidance on the law and personal data, including your rights and how to access your personal information.

<http://www.ico.org.uk>

Health Research Authority: The HRA protects and promotes the interests of patients and the public in health and social care research.

<http://www.hra.nhs.uk>

Appendix A

Activity	Rationale
Quality monitoring, concerns and serious incidents	<p>Purpose – We need to ensure that the health services you receive are safe, effective and of excellent quality. Sometimes concerns are raised about the care provided or an incident has happened that we need to investigate. You may not have made a complaint to us directly but the health care professional looking after you may decide that we need to know in order to help make improvements.</p> <p>Legal Basis - SHCP We have a statutory duty under the Health and Social Care Act 2012, Part 1, Section 26, in securing continuous improvement in the quality of services provided. and will rely on your explicit consent as the basis to undertake such activities.</p> <p>Data Processor – We process this information ourselves.</p>
Freedom of Information (FOI) requests	<p>Purpose – To process personal information in relation to FOI requests made by an individual to enable response to be provided.</p> <p>Legal Basis – FOI Act.</p> <p>Data Processor – We process this information ourselves.</p>
Individual Funding Requests (IFR)	<p>Purpose – We may need to process and share your personal information with the IFR team for the funding of treatment that is not normally covered in the standard contract.</p> <p>Legal Basis – The clinical professional who first identifies that you may need</p>



	<p>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.</p> <p>Data processor – NHS Surrey Downs CCG to do this on behalf of Surrey Heath CCG.</p>
Safeguarding	<p>Purpose – Safeguarding means protecting peoples' health, wellbeing and human rights, and enabling them to live free from harm, abuse and neglect. It is a key part of providing high-quality health and social care. SHCP will participate in Serious Case Reviews undertaken by either the local Children's Safeguarding Boards or the Adult Safeguarding Boards for continued learning, to minimize risk and to improve services.</p> <p>Legal Basis - SHCP has a statutory responsibility under the Children Act 2004, Care Act 2014 and safeguarding provision within the Data Protection Act 2018 – Schedule 1, Part 2, subsections 18 and 19 to ensure the safety of all children, and the safety of adults at risk of abuse and neglect.</p> <p>Data Processor – We may undertake these ourselves or refer you to the local CCG.</p>
Patient and Public Involvement	<p>Purpose – If you have asked us to keep you regularly informed and up to date about the work of SHCP or if you are actively involved in our engagement and consultation activities or patient participation groups, we will collect and process data which you have agreed to share with us.</p> <p>Where you submit your details to us for involvement purposes, we will only use your information for this purpose. You can opt out at any time by contacting us using our contact details at the end of this document.</p> <p>Legal Basis - Explicit consent is used for this purpose.</p> <p>Data Processor – We process this information ourselves.</p>
Commissioning, planning and contract monitoring	<p>Purpose – To collect NHS data about services we have commissioned to provide services to you. We also work with other local CCG's, and GP Federations and often hold joint contracts and commission joint services to make best use of the money available to us.</p> <p>We set our reporting requirements as part of our contracts with NHS service providers and do not ask them to give us identifiable data about you.</p> <p>Legal Basis - Our legal basis for collecting and processing information for this purpose is statutory under the Health & Social Care Act 2012 chapter A2 establishment and duties.</p> <p>Data Processor – We process this information ourselves</p>
Infection Control	<p>Purpose</p> <p>SHCP has an obligation for carrying out Infection Control surveillances. This work is undertaken by a clinical member of Staff with support from Practices</p>



	<p>and Acute Trusts to provide the relevant information for the investigation to be undertaken and outcomes derived.</p> <p>Legal Basis</p> <p>The Health Service (Control of Patient Information) Regulations 2000. Paragraph 3 enables the lawful processing of patient information in relation to diagnosing, recognising trends, controlling, preventing, monitoring and managing communicable diseases and other risks to public health.</p> <p>http://www.legislation.gov.uk/uksi/2002/1438/made?view=plain</p> <p>Mandatory Health Care Associated Infection Surveillance: Data Quality Statement April 2016 (PHE)</p> <p>Benefits</p> <p>The surveillance reports produces actions and lessons learnt that both support direct improved care of patients but also to continuously improve the safety of patients and be focused on clinical learning.</p> <p>Data Processor – We process this information ourselves</p>
Cabinet Office	<p>Purpose</p> <p>The Cabinet Office is responsible for carrying out data matching exercises. Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.</p> <p>We participate in the Cabinet Office’s National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise, as detailed here.</p> <p>Legal Basis</p> <p>The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014. It does not require the consent of the individuals concerned under GDPR.</p> <p>Data matching by the Cabinet Office is subject to a Code of Practice.</p> <p>View further information on the Cabinet Office’s legal powers and the reasons why it matches particular information.</p> <p>https://www.gov.uk/government/publications/code-of-data-matching-practice-for-national-fraud-initiative</p>
National Registries	National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service



	<p>user identifiable information without the need to seek informed consent from each individual service user.</p>
Research	<p>Purpose – Data may be collected for the purpose of research.</p> <p>Research can be undertaken using information that does not identify you (anonymised). The law does not require your consent to be obtained in this case but information should be made available to you where your anonymised data is used for the purposes of research. Information can be made available either in waiting rooms, using information leaflets, published on notice boards, waiting room screens and/or an organisations website.</p> <p>Where identifiable data is needed for research, you may be approached by an organisation who has provided you with care and asked if you wish to participate in a research study. Where identifiable data is required, an organisation must obtain explicit consent. A member of the research team will discuss the research study with you and will provide you with information on what the study is about, what information they wish to collect, how to opt out and who to contact for more information.</p> <p>If you do not wish your information to be used for research, whether identifiable or non-identifiable, please let your GP Practice know. They will add a code to your records that will stop your information from being used for research.</p> <p>Legal Basis – Your consent will be obtained by the organisation holding your records before identifiable information about you is disclosed for any research. If this is not possible then the organisation wishing to use your information will need to seek formal approval from the Confidentiality Advisory Group (CAG). For further information please visit the NHS Health Research Authority website https://www.hra.nhs.uk/.</p>
Clinical Commissioning Groups	<p>Activities – Contract monitoring and commissioning of services</p> <p>Legal Basis – NHS Act 2006 & Health and Social Care Act 2012</p>
Surveys and asking for your feedback	<p>Sometimes we may offer you the opportunity to take part in a survey that the practice is running. We will not generally ask you to give us any personal confidential information as part of any survey.</p> <p>Legal Basis – you are under no obligation to take part and where you do, we consider your participation as consent to hold and use the responses you give us.</p> <p>Data Processor – Survey Monkey</p>
Extended hours	<p>Purpose – To provide additional clinical appointment to the population with the geographical area of Surrey Heath.</p> <p>Legal Basis – Direct Care (Data Protection Legislation, Article 6 1(3) & 9 2(h)</p> <p>Data Processor – Surrey Heath GP Practices are contracted to provide the additional hours on Saturdays, NHUC are contracted by SHCP to provide the</p>



	additional hours during Sunday opening
Acute and Community Providers	<p>Purpose – To improve the health outcomes of patients SHCP receives data and information from various Controllers in the Acute and Community environment, including but not limited to Frimley Heath Foundation Trust, Surrey and Borders, and Clinical Partners.</p> <p>Legal Basis – Direct Care (Data Protection Legislation, Article 6 1(3) & 9 2(h))</p> <p>Data Processor – We process this information ourselves</p>
Pharmacists	<p>Purpose – to provide monitoring and advice in line with the national directive for prescribing to GP Practices. Anonymous data is collected by SHCP.</p> <p>Legal Basis – Direct Care (Data Protection Legislation, Article 6 1(3) & 9 2(h))</p> <p>Data Processor – We do this ourselves using GP systems.</p>
National Registries	National Registries (such as the Learning Disabilities Register) have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.
Public Health England	<p>Purpose – National objective to improve health outcomes of patients in the UK nad to communicate communicable diseases.</p> <p>Legal Basis – Direct Care (Data Protection Legislation, Article 6 1(3) & 9 2(g & h))</p> <p>Data Processor – Public Health England</p>
Other organisations who provide support services for us	<p>Purpose –SHCP will use the services of additional organisations (other than those listed above), who will provide additional expertise to support the work of the CCG.</p> <p>Legal Basis - We have entered into contracts with other organisations to provide some services for us or on our behalf. These organisations may process or be in the vicinity of SHCP data and could be identified as ‘processors’. Information that we may hold about you will not be shared or made available to any of these organisations. Below are their details and a brief description of the functions they carry out on our behalf:</p> <p>IRIS – Provide Payroll services to SHCP</p> <p>Peninsular – Provide HR and Health and Safety services to SHCP</p> <p>SCW – Provide training services to SHCP</p> <p>Brewers – Provide accounting service to SHCP</p> <p>For further details, please contact SHCP.</p>



OFFICIAL



	http://www.surreyheathcommunityproviders.co.uk/contact/
--	---