

Fair Processing Notice (Privacy Notice)

Your Personal Information – what you need to know

Who we are and what we do

NHS Surrey Heath Clinical Commissioning Group (CCG) is responsible for securing, planning, designing and paying for your NHS services, including planned and emergency hospital care, as well as community and primary medical care (GP) services. 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. This is known as commissioning. For further information please refer to the 'About Us' page on our Website:

<http://www.surreyheathccg.nhs.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.

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..

NHS Surrey Heath CCG is a Data Controller as defined under the GDPR. We are legally responsible for ensuring that all personal information that we process i.e. hold, obtain, record, use or share about you, is done in compliance with the six Data Protection Principles as set out in Article 5 under GDPR.

All data controllers must notify the Information Commissioner's Office (ICO) of all personal information processing activities. Our ICO Data Protection Registration number is A8265660 and our entry can be found in the Data Protection Register on the Information Commissioner's Office website

Everyone working for the NHS has a legal duty to keep information about you confidential. The NHS Care Record Guarantee and NHS Constitution provide a commitment that all 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.

If you are receiving services from the NHS, we share information that does not identify you (anonymised) with other NHS and social care partner agencies for the purpose of improving local services, research, audit and public health.

The CCG is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.

All information that we hold about you will be held securely and confidentially. We use administrative and technical controls to do this. We use strict controls to ensure that only a limited number of authorised staff are able to see information that identifies you. Only a limited number of authorised staff have access to information that identifies you where it is appropriate to their role and is strictly on a need-to-know basis.

All of our staff, contractors and committee members receive role appropriate and on-going training to ensure they are aware of their personal responsibilities and have contractual obligations to uphold confidentiality, enforceable through disciplinary procedures.

We will only use the minimum amount of information necessary about you.

We will only retain information in accordance with the schedules set out in the Records Management Code of Practice.

What kind of information do we use?

As a Commissioner we do not routinely hold or have access to your medical records. However, we may need to hold some personal information about you, for example:

- Your name, address, your date of birth, contact details and your NHS number which in some circumstances we may use as your single identifying number with no other information about you attached. Your NHS number is present in all of your health records and therefore we are able to use that number to link information to you or about you without revealing any personal or confidential data, where we are lawfully allowed to do this.
- Details of your GP, what treatment you have received and where you received it
- Details of concerns or complaints you have raised about your healthcare provision and we need to investigate
- Details of clinical concerns raised by your General Practitioner (GP) or service providers about your healthcare provision
- If you ask us for our help or involvement with your healthcare, or where we are required to fund specific specialised treatment for a particular condition that is not already covered in our contracts with organisations that provide NHS care
- If you ask us to keep you regularly informed and up-to-date about the work of the CCG, or if you are actively involved in our engagement and consultation activities or service user/Patient Participation Groups

Our records may include relevant information that you have told us, or information provided on your behalf by relatives or those who care for you and know you well, or from health professionals and other staff directly involved in your care and treatment. Our records may be held on paper or in a computer system.

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. Article 4 of the GDPR
- 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. Article 9 of the GDPR
- 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 – this is data that has undergone a technical process that replaces your identifiable information such as NHS number, postcode, date of birth with a unique identifier, which obscures the 'real world' identity of the individual patient to those working with the data
- Anonymised – this is data about individuals but with identifying details removed so that there is little or no risk of the individual being re-identified
- Aggregated – anonymised information that is grouped together so that it doesn't identify individuals

What do we use your personal and special categories of personal data for?

There are some limited exceptions where we may hold and use personal data and special categories of personal data about you. For example the CCG is required by law to perform certain services that involve the processing of these data types.

The areas where we regularly use personal data and special categories of personal data include:

- responding to your queries, compliments or concerns

- assessment and evaluation of safeguarding concerns

We may also use this data in the following cases:

- the information is necessary for your direct healthcare needs
- we need to respond to patients, carers or Member of Parliament communications
- you have freely given your explicit agreement (consent) for us to use your information for a specific purpose
- there is an overriding public interest in using the information e.g. in order to safeguard an individual, or to prevent a serious crime
- there is a legal requirement that will allow us to use or provide information (e.g. a formal court order).

What do we use non-identifiable data for?

We use pseudonymised, anonymised and aggregated data to plan health care services. Specifically we use it to:

- check the quality and efficiency of the health services we commission
- prepare performance reports on the services we commission
- work out what illnesses people may have in the future, so we can plan and prioritise services and ensure these meet the needs of patients in the future
- review the care being provided to make sure it is of the highest standard
- Evaluate the services we have or have been commissioned on our behalf
- To support the regional and national initiatives through the Integrated Care Systems (ICS) or the Sustainability and Transformation Plan (STP)

Do we share your information with other organisations?

We commission a number of organisations (both within and outside the NHS) to provide healthcare services to you. We may also share anonymised and aggregated statistical information with them for the purpose of improving local services, research, audit and public health; for example understanding how health conditions spread across our local area compared against other areas.

We work in collaboration with other Commissioners and as part of the Frimley ICS to jointly commission services across Surrey and Hampshire. These require the inter-sharing of statistical information for the purposes of improving those services commissioned and the health outcomes of our population.

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

- You have given us explicit consent;
- 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 there is an overriding public health interest e.g. communicable diseases as instructed by NHS England
- When permission is given by the Secretary of State or the Health Research Authority on the advice of the Confidentiality Advisory Group to process personal and special categories of personal data without the explicit consent of individuals

The Health and Social Care Act 2012 provides some NHS bodies, particularly NHS Digital (formally the Health and Social Care information Centre) ways of collecting and using patient data that cannot identify a person to help Commissioners to design and procure the combination of services that best suit the population they serve.

How we process information within the CCG

The CCG contracts with other organisations to process data on our behalf. These organisations are known as 'Processors' and we ensure they are legally and contractually bound, providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the General Data Protection Regulation (GDPR) and ensure the protection of the rights of the data subject.

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

When analysing current health services and proposals for developing future services it is sometimes necessary to link separate individual datasets to be able to produce a comprehensive evaluation. This may involve linking primary care data from your Doctor (GP) with other data such as hospital inpatient stays, outpatient appointments and A&E attendances; this type of data is called secondary uses service (SUS) data. In some cases there may also be a need to link local datasets which could include a range of other hospital based services such as radiology, physiotherapy, audiology etc., as well as mental health and community-based clinics and services such as district nursing, podiatry etc. When carrying out this analysis, the linkage of these datasets is always done using a pseudonym (unique identifier), applied by NHS Digital, that does not reveal a person's identity as the CCG does not have any access to identifiable data for these purposes.

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.

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

We only use information that may identify you in accordance with the data protection legislation (as defined in the Data Protection Act 2018). The data protection legislation requires us to process personal data only if there is a legitimate/legal basis for doing so and that any processing must be fair, lawful and transparent.

Within the health sector, we also have to follow the common law duty of confidentiality, 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.

Everyone working for the NHS has a legal duty to keep information about you confidential. The NHS Care Record Guarantee and NHS Constitution provide a commitment that all 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.

The [Confidentiality: NHS Code of Practice](#) applies to all of our staff, and they 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. All CCG staff are expected to make sure information is kept confidential and receive annual training on how to do this. This is monitored by the CCG 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 masks data so that unauthorised users cannot see or make sense of it).

We ensure external data processors that support us are legally and contractually bound to operate and prove security arrangements are in place where data that could or does identify a person are processed.

Accountability

The CCG has a senior member of staff responsible for protecting the confidentiality of patient information. This person is called the Caldicott Guardian. The contact details of our Caldicott Guardian are as follows:

Dr John Fraser
Tel: 01276 707572
Email: John.Fraser4@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:

Robert Morgan – Chief Finance Officer
Tel: 01276 707572
Email: Robert.Morgan2@nhs.net

The CCG has a Data Protection Officer (DPO) responsible for; monitoring compliance with the GDPR and other data protection legislation, Information Governance (IG) policies, providing advice and guidance, raising awareness, training and audits. The DPO acts as a contact point for the ICO, our 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: 01276 707572

Email: DPO.SHCCG@nhs.net

The CCG is registered with the Information Commissioner's Office (ICO) as a data controller and collects data for a variety of purposes. Our registration number is **Z3628479** and a copy of the registration is available through the [ICO website](#).

How long do we hold information for?

The CCGs approach to the management of its business records are in line with national guidance from NHS Digital, [Records Management Code of Practice](#). The code of practice sets out the best practice for NHS organisations to follow. To ensure compliance the CCG's records shall not be retained indefinitely and 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. Confidential information (whether personal or commercially) will be disposed of by approved and secure confidential waste procedures. We keep a record of retention schedules within our information asset registers.

Your right to opt out of data sharing and processing

The NHS Constitution states 'You have a right to request that your personal confidential information is not used beyond your own direct care and treatment and to have your objections considered'. For further information please visit: <https://www.gov.uk/government/publications/the-nhs-constitution-for-england>

Direct care is defined as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation or suffering of an individual.

Indirect care is defined as work within the health and social care environment which does not involve the direct treatment or support of individuals e.g. research, commissioning and much of the work done in public health.

There are several forms of opt- outs available at different levels. These include for example:

Information directly collected by the CCG. Your choices can be exercised by withdrawing your consent for the sharing of information that identifies you, unless there is an overriding legal obligation. We will first need to explain how this may affect the care you receive but you can do this by writing to us.

Information not directly collected by the CCG but collected by organisations that provide NHS services. These are known as Type 1 and National data opt-outs (previously Type 2) and are described below:

Type 1 opt-out.

If you do not want personal confidential information that identifies you to be shared outside your GP practice, for purposes beyond your direct care, you can register a 'Type 1 Opt-Out' with your GP practice. This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Patients are only able to register an opt-out at their GP practice.

Records for patients who have registered a 'Type 1 Opt-Out' will be identified using a particular code that will be applied to your medical records that will stop your records from being shared outside of your GP Practice.

National data opt-out

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](#)

The use of personal confidential data by CCGs for invoice validation under approval reference (CAG 7-07)(a-c)/2013) has been recently extended to the end of September 2020 [NHS England Invoice Validation](#) and as part of that review, it has been agreed that NO opt out will be applied to invoice validation due to the importance of accurately allocating NHS resources and the lack of evidence of public concern in relation to the use of data for this specific purpose. This effectively means that data which includes an identifier (usually NHS number) which is flowing from NHS Digital to commissioners for invoice validation/challenge purposes will be provided for all patients to ensure that providers receive the correct funding for the health and care services they provide.

To find out more visit the NHS Digital website <https://digital.nhs.uk/opting-out>

Gaining access to the data we hold about you

Exercising the Right of Access (Subject Access Requests)

Individuals can find out if we hold any personal information by making a request under the Right of Access under the GDPR, more commonly called a 'Subject Access Request' under the GDPR. If we do hold information about you we will.

- Give you a description of it;
- Tell you why we are holding it;
- Tell you who it could be disclosed to;
- Let you have a copy of the information in an intelligible form; and
- Correct any mistakes to information held

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, but you may be charged a fee.

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 corporate policies page on our website - <http://www.surreyheathccg.nhs.uk/policies-publications/corporate-policies>

If you require further advice you can contact us on: 01276 707572 or via email: SHCCG.ContactUs@nhs.net or put your request in writing to:

By post: NHS Surrey Heath Clinical Commissioning Group
Surrey Heath House
Knoll Road
Camberley
Surrey
GU15 3HD

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 or information that is covered by

the data protection legislation under FOIA. However you can request this under a Subject 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: scwcsu.surreyheathccg@nhs.net

By post: Freedom of Information
NHS Surrey Heath CCG
Surrey Heath House
Knoll Road
Camberley
GU15 3HD

For further information please visit the CCG’s FOI page on our website;
<http://www.surreyheathccg.nhs.uk/contact/freedom-of-information>

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: 01276 707572

By email: SHCCG.CommentsandComplaints@nhs.net

By post: Comments & Complaints Team
NHS Surrey Heath CCG
Surrey Heath House
Knoll Road
CAMBERLEY
Surrey
GU15 3HD

For further information go to: <http://www.surreyheathccg.nhs.uk/contact>

Your Rights

GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling.

Overseas Transfers

Your information will not be sent outside of the EEA where the laws do not protect your privacy to the same extent as the law in the UK and or in compliance with the General data Protection Regulation. We will never sell any information about you.

Automated Decision Making

The CCG will not make decisions based solely on automated processing

Links to other websites

This Fair Processing Notice does not cover the links within CCG's website 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 May 2018.

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
Complaints	<p>Purpose – To process your personal information if it relates to a complaint where you have asked for our help or involvement. For contact details please see the CCG’s contact us webpage http://www.surreyheathccg.nhs.uk/contact</p> <p>Legal Basis - The CCG has a duty as to the improvement in quality of services under Section 14R NHS Act 2006 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. For further information please visit the CCG’s FOI page on our webpage http://www.surreyheathccg.nhs.uk/contact/freedom-of-information</p> <p>Legal Basis – FOI Act.</p> <p>Data Processor – We ask SCW CSU to process requests on our behalf.</p>
Individual Funding Requests	<p>Purpose – We may need to process your personal information where we are requested to fund specific treatment for you for a particular condition that is not already covered in our contracts.</p> <p>Legal Basis –The National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012 part 7 (34) sets out the duty of a CCG in regards to funding and commissioning of drugs and other Treatments. The clinical professional who first identifies that you may need the treatment will explain to you the information that is needed to be collected and processed in order to assess your needs and commission your care; they will gain your explicit consent to share this.</p> <p>Data processor – We ask NHS Surrey Downs CCG to do this on our behalf.</p>
Continuing Healthcare (CHC)	<p>Purpose – We may need to process your identifiable information where you have asked for an assessment for Continuing Healthcare funding (a package of care for those with complex medical needs) and you need to have a particular care package commissioned for you.</p> <p>Legal Basis - The National Health Service Commissioning Board and Clinical Commissioning Groups (Responsibilities and Standing Rules) Regulations 2012 section part 6 sets out the duty of a CCG in regards to the assessment and provision of NHS Continuing Healthcare. The clinical professional who first sees you to discuss your needs will explain to you the information that they need to collect and process in order for your needs to be assessed and commission your care; they will gain your explicit consent to share this.</p> <p>Data Processor – we ask NHS Surrey Downs CCG to undertake assessments and commission your care on our behalf.</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. The CCG will participate in Serious</p>

	<p>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 - The CCG 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 ask NHS Guildford and Waverley CCG to undertake assessments and commission your care on our behalf.</p>
Invoice Processing	<p>Purpose – The Invoice Validation process ensures that care providers who provide you with care and treatment can be paid for the services they provide in a timely and efficient manner.</p> <p>There are situations where personal data is required to ensure that the correct service provider is paid.</p> <p>In such cases service providers are required to send identifiable patient personal identifiable data such as NHS Number to a Controlled Environment for Finance (CEfF) which is a secure restricted area within SCWCSU who process this data on our behalf and indicate which invoices we can validate (authorize) for payment.</p> <p>NHS England has published guidance on how invoices must be processed and Commissioners have a duty to detect report and investigate any incidents of where a breach of confidentiality has been made. For more information see: https://www.england.nhs.uk/ourwork/tsd/ig/in-val/invoice-validation-faqs/</p> <p>NHS SBS do not require and should not receive any personal data to provide their services.</p> <p>Type of Data – Confidential Information/Special Category/Identifiable/Pseudonymised/Anonymised</p> <p>Legal Basis - GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of personal confidential data by CCGs for invoice validation has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-07)(a-c)/2013)) and this approval has been extended to the end of September 2020 NHS England Invoice Validation which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for invoice validation purposes which sets aside the duty of confidentiality. We are committed to conducting invoice validation effectively, in ways that are consistent with the laws that protect your confidentiality.</p> <p>Data Processors - NHS Shared Business Services (SBS) and NHS South Central and West Commissioning Support Unit (CSU) process invoices on behalf of the 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 the CCG 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 - Under the NHS Act 2006 Section 14Z2, the CCG has a duty, in relation to health services provided (or which are to be provided) under arrangements made by</p>

	<p>the CCG exercising its functions, to make arrangements so as to secure that individuals to whom the services are being (or may be) provided are involved at various specified stages. We will rely on your explicit consent for this purpose.</p> <p>Data Processor – We process this information ourselves.</p>
<p>Quality monitoring, concerns and serious incidents</p>	<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 – The health care professional raising the concern or reporting the incident should make every attempt to talk to you about this and gain your consent to share information about you with us. Sometimes they can do this without telling us who you are. 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.</p> <p>Data processor – We process data given to us by GP’s and other health care professionals that may include details of the care you have received and any concerns about that care. In order to look into these concerns we may need to talk to other organisations such as other local CCGs as well as other Public bodies and Government agencies such as NHS Improvement, the Care Quality Commission, NHS England as well as the Providers of your care.</p>
<p>Commissioning, planning and contract monitoring</p>	<p>Purpose – To collect NHS data about services we have commissioned to provide services to you. We also work with other local CCGs 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 – NHS Digital collect various data sets from NHS service providers that have been agreed locally. All identifying information about you is removed by NHS Digital before the information is made available for the CCG to monitor and manage its contracts. We also have signed a Data Sharing Framework and Data Sharing Agreement with NHS Digital and have been given approval to use a wide range of data to help us commission care services. This agreement makes sure that we only process data that does not identify you, that we keep the information secure and we do not share it without the agreement of NHS Digital. For more information about the types of data that NHS Digital collect please use this link http://digital.nhs.uk/datasets.</p> <p>NHS South Central and West Commissioning Support Unit (CSU) & North East London CSU provide analytical Business Intelligence support on our behalf.</p>
<p>Integrated Care</p>	<p>Purpose – The Integrated Care Team (ICT) has been developed to provide a better experience for you and your carers if you have complex health and social care needs. A jointly managed integrated care plan will be developed to ensure that your care is managed more effectively.</p> <p>This is achieved by an integrated care management team, meeting to establish how they can work together most effectively with you to provide your care. You will be</p>

	<p>involved in these discussions and will receive a copy of your integrated care plan.</p> <p>To achieve the best care for you, your integrated care plan will be shared with other organisations that you may come into contact with, for example, the GP out of hour's service, the local acute hospitals and others as applicable. These organisations may not be involved with your care currently but by sharing your integrated care plan with them they will be able to recognise that you are receiving integrated care should you need to contact them. Your integrated care plan will therefore be shared electronically with all of the organisations included in your consent form.</p> <p>Legal Basis – Under the NHS Act 2012 14Z1, states the CCG has duty as to promoting integration and must exercise its functions with a view to securing that health services are provided in an integrated way .The clinical professional who first sees you to discuss your needs will explain to you the information that they need to collect and process in order for your needs to be assessed and commission your care; they will gain your explicit consent to share this and refer to into the ICT.</p> <p>Data Processor – The staff who work in the Integrated Care Teams will jointly process your health and care data with the organisations involved in your care. http://www.surreyheathccg.nhs.uk/integration-of-care</p>
<p>Risk Stratification</p>	<p>Rationale</p> <p>Risk stratification is a process that uses de-identified personal data from health care services to determine which people are at risk of experiencing certain outcomes, such as unplanned hospital admissions.</p> <p>Data Processing activities for Risk Stratification</p> <p>Risk stratification tools are used by CCGs to analyse the overall health of a population using data which is anonymised in line with the Information Commissioner's Office (ICO) Anonymisation Code of Practice. The combined CCGs Secondary Use Service (SUS) data and GP data which contains an identifier (usually NHS number) is made available to clinicians with a legitimate relationship with their patients to enable them to identify which patients should be offered targeted preventative support to reduce those risks.</p> <p>The CCG has commissioned NHS South, Central and West Commissioning Support Unit (SCWCSU) to provide the risk stratification software solution on behalf of itself and its GP practices.</p> <p>This processing takes place under contract following the below steps:</p> <ul style="list-style-type: none"> • NHS Digital has a legal obligation to obtain data from providers of NHS care such as the local hospital or community hospital. This data is then sent to the SCWCSU DSCRO and amended so that only your NHS number could identify you. The data is then provided to SCWCSU for processing in the risk stratification software. The CCG has signed a Data Sharing Contract with NHS Digital for the use of this data, called Secondary Use Services (SUS) data. • Your GP practice enables an organisation called Graphnet Healthcare, to extract data from your records which again, is only identifiable by your NHS Number. This data will only be extracted and provided to SCWCSU for those patients that have not objected to Risk Stratification or where no other type of objection to information sharing has been recorded on

	<p>your record. The data, containing the same verified NHS numbers, are sent via secure transfer, directly to SCWCSU by Graphnet.</p> <ul style="list-style-type: none"> • SCWCSU then link both sets of data using their risk stratification software. An algorithm is run on the data to generate a risk score for each Patient. The CCG is able to see data only after your NHS number has been removed and replaced by a pseudonymised reference. Your GP will be able to see the data with your NHS number in it so that it can identify if you require further support from them to manage your healthcare needs. <p>The risk scores are <i>only</i> made available to authorized users within the GP Practice where you are registered via a secure portal managed by SCWCSU.</p> <p>If you do not wish information about you to be included in the risk stratification programme please contact your GP Practice. They can add a code to your records that will stop your information from being used for this purpose.</p> <p>Further information about risk stratification is available from: https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/</p> <p>Type of Data – Identifiable/Pseudonymised/Anonymised/Aggregate Data</p> <p>Legal Basis</p> <p>GDPR Art. 6(1) (e) and Art.9 (2) (h). The use of identifiable data by CCGs and GPs for risk stratification has been approved by the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority (approval reference (CAG 7-04)(a)/2013)) and this approval has been extended to the end of September 2020 NHS England Risk Stratification which gives us a statutory legal basis under Section 251 of the NHS Act 2006 to process data for risk stratification purposes which sets aside the duty of confidentiality. We are committed to conducting risk stratification effectively, in ways that are consistent with the laws that protect your confidentiality.</p> <p>Benefits</p> <p>CCGs and GPs use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions. Typically this is because patients have a long term condition such as Chronic Obstructive Pulmonary Disease. NHS England encourages CCGs and GPs to use risk stratification tools as part of their local strategies for supporting patients with long-term conditions and to help and prevent avoidable admissions.</p> <p>Knowledge of the risk profile of our population will help the CCG to commission appropriate preventative services and to promote quality improvement in collaboration with our GP practices.</p>
Cabinet Office	<p>Purpose – 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</p>

	<p>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 –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	<p>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.</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>

<p>Commissioning Support</p> <p>South Central and West CSU</p> <p>NHS Digital DSCRO</p> <p>Optum Health Solutions (UK) Ltd</p>	<p>Purpose -The CCG will use other organisations to provide us with support services. These organisations will process information on our behalf. These organisations are known as “data processors” and will provide additional expertise to support the work of CCG:</p> <p>Legal Basis - The CCG are committed to ensure that a legal basis is identified for all flows of personal identifiable to external organisations.</p> <p>The CCG ensures that this is supported by use of an NHS Standard Contract which is mandated by NHS England for use by commissioners for all contracts for healthcare services other than primary care.</p> <p>Activities – Undertakes the processing of pseudonymised SUS data and local data flows to provide contract management for the services commissioned by the CCG, other than those identified above with the applicable legal basis</p> <p>Legal Basis - GDPR & Data protection Act, S251 NHS Act 2006 & Health and Social Care Act 2012</p> <p>Activities – Undertakes the processing of identifiable Secondary Use Service (SUS) data and local data flows to provide speudonymised commissioning data to the CCG’s ‘processors’.</p> <p>Legal Basis - NHS Act 2006 & Health and Social Care Act 2012</p> <p>Activities - Undertakes the processing of pseudonymised SUS data and local data flows to provide contract management for London Providers commissioned by the group of CCGs known as The London Focus Group</p> <p>Legal Basis - GDPR & Data Protection Act, S251 NHS Act 2006 & Health and Social Care Act 2012</p>
<p>Other organisations who provide support services for us</p>	<p>Purpose -The CCG 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 CCG 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>TIAA – Provide internal audit services for the CCG</p> <p>Grant Thornton – Provide external audit services for the CCG</p> <p>KPMG – Provide external audit services for the CCG</p> <p>Surrey County Council - We ask the Council to provide facilities and building Services to the CCG as we share a building with them.</p> <p>For further details, please contact the CCG.</p> <p>http://www.surreyheathccg.nhs.uk/contact</p>