NHS
Surrey Heartlands
Clinical Commissioning Group

# How we use your information

## Introduction

The purpose of this notice is to inform you of the way in which we, NHS Surrey Heartlands Clinical Commissioning Group, use information (including personal data) about you. In this notice we will explain:

- Who we are and what we do;
- The types of information we hold about people;
- How we use this information and why we need to do this;
- Who we may share your information with;
- How you can object to the way we use information or complain about this;
- How you can access a copy of the information we hold about you;
- What other rights you may have in relation to this information;
- How we keep your information secure and confidential;
- Where to go if you require further information.

This guidance applies to all individuals whose information is used by the CCG; including local NHS service users, our staff and suppliers, and visitors to our offices.

This information is sometimes known as a 'Privacy Notice' or 'Fair Processing Notice' and it is a legal obligation under data protection legislation that we provide you with this.

We will review this information regularly and update it as required - so we would recommend that you check this webpage regularly to ensure that you remain informed about the way in which we use your information.

## Who we are

This notice applies to NHS Surrey Heartlands CCG (the CCG) only. CCGs were established under the Health and Social Care Act 2012 to commission (buy) a range of health and social care services to meet the needs of local areas. We also monitor the performance of these services to ensure that they offer the highest quality of healthcare. You can find out more about us and the work that we do from our website.

The CCGs that operate within Surrey have agreed to work collaboratively to commission Surrey-wide services for patients. Please see our website for further information regarding Surrey CCG Collaborative commissioning arrangements. The CCG is also part of the Surrey Heartlands Integrated Care System.

The CCG is usually the Data Controller for your information that we hold and this means that we are the legal entity that is responsible for determining how this will be used and ensuring that this use complies with applicable data protection legislation. Where we are working collaboratively with another CCG we may be joint data controllers for your information.

The CCG is registered with the Information Commissioner's Office (ICO) as a Data Controller – please see the ICO's public register for further information.

**What we do**

The Health and Social Care Act 2012 gives the CCG a range of duties and powers (please see link for further guidance) and in accordance with these the CCG undertakes the following activities:

- Commissioning of Primary Care services provided by GP Practices (under delegated authority from NHS England)
- Commissioning of Secondary Care Services provided by Hospitals (Acute Trusts), Community Health Services, and also Mental Health Services
- Monitoring the quality of commissioning services and dealing with concerns from service users
- Medicines Management, including authorisation for controlled drugs
- Governance and administration duties to ensure that we are a well-managed organisation
- Providing services to other health care organisations (including support with Medicines Management reviews, Business Intelligence, and Emergency Planning Resilience & Response related activities etc.)
- Operating a Primary Care Referral Support Service for GP Practices
- Assessing Individual Funding Requests (Surrey-wide service provided by the CCG)
- Managing Continuing Healthcare for adults (Surrey-wide service provided by the CCG)
- Managing Continuing Healthcare for children (Surrey-wide service provided by the CCG)
- Safeguarding vulnerable adults and children (Surrey-wide service provided by the CCG)
- Operating a Patient Emergency Transport and Out of Hours Care (Surrey-wide service)

**Whose information we hold**

To allow us to undertake the activities above we will use information relating to the following types of people:

- people who use the services we commission;

- individuals undertaking work for commissioned providers organisations, other health and social care organisations with which we work, and suppliers of goods and services;
- people who undertake work for us, or have applied to do so.

**What types of information we use**

To allow us to undertake the activities above we will use different types of information, this includes:

- ***Identifiable Personal Data*** – you can easily be identified from this information, which relates to you. We will only use this where there is no other viable alternative. Identifiable personal data includes:
  - ***Personal Data*** (for example your name, contact details, or date of birth)
  - ***Special Categories of Personal Data*** (which includes data relating to ethnicity, sexual orientation, and also data relating to physical or mental health)
- ***Non-Identifiable Personal Data*** – this includes '***Pseudonymised Personal Data***' where personal data which could be used to identify you has been replaced with a pseudonym. It also includes personal data which is classed by the NHS as '***Anonymised in Context'*** as it includes a local identifier, such as your hospital number. This information could potentially be used to identify you, if it was processed outside of the CCG and/or added to other information, so we ensure that we have robust controls in place to manage how this is used;
- ***Anonymised Data*** – you cannot be identified from this, even if it is added to other information.

**How the CCG gets this information**

We generally receive information about people in one of the following ways:

- The person it relates (e.g. a service user or staff member) or their authorised representative provides it to us directly;
- We receive it from another health and social care organisation with which we work;
- It is provided to us via NHS Digital or directly by one of our commissioned providers if it is Non-Identifiable Personal Data that relates to CCG commissioned services.

**Why we use this information**

We use different types of information for different purposes as detailed below:

- To undertake our ***commissioning and planning*** activity we will use Anonymised Data wherever appropriate or Non-Identifiable Personal Data

where we require this to be able to undertake detailed work and to be able to link data together;

- To ***provide or support direct healthcare*** we will seek to use Non-Identifiable Personal Data wherever this is possible however we may need to use Personal Data and Special Categories of Personal Data, such as information relating to physical or mental health, to ensure that risks to patient safety are minimised;
- For ***regulatory and public health functions*** we will seek to use Non-Identifiable Personal Data wherever this is possible however we may need to use Personal Data and Special Categories of Personal Data, such as information relating to physical or mental health, to ensure that risks to public health are minimised;
- For ***safeguarding*** activity we will use Personal Data and Special Categories of Personal Data, such as information relating to physical or mental health, to ensure that risks to individuals are minimised;
- To fulfil our ***statutory duties*** under various pieces of applicable legislation and to undertake ***employment related activities*** we need to process personal data and Special Categories of Personal Data; such as data relating to ethnicity, gender, and sexual orientation etc. This will also require that we process data relating to criminal convictions relating to individuals wo are undertaking work for us or applying to do so;
- To be a well-managed organisation, and fulfil ***governance and administration responsibilities***, we may need to process personal data and, occasionally, Special Categories of Personal Data.

**The lawful basis for this activity**

Data protection legislation requires that we explain the lawful basis for us processing personal data. The CCG has undertaken detailed reviews and has identified that the activity involving personal data we carry out will be lawful under data protection legislation because either:

- it is necessary for performance of a task carried out in the public interests or in the exercise of ***official authority*** as CCGs have a statutory duty or power to do this under the NHS Act 2006, Health & Social Care Act 2012 or another applicable piece of legislation;
- it is necessary for the performance of a ***contract*** to which a person is party or in order to take steps at the request of a person prior to entering into a contract;
- we hold the documented, informed ***consent*** of the person to use their data in this way;
- it is necessary for us to comply with a ***legal obligation*** that we are subject to;
- it is necessary for the ***legitimate interests*** of the CCG (this does not include any personal data processed for the purposes of meeting our statutory

duties). The CCG believes that we have legitimate interests in ensuring strategic alignment and the best possible use of public funds.

Where individuals undertaking work for the CCG are legitimately required to process Special Categories of Personal Data as part of their responsibilities this will also be lawful as this activity will be either:

- undertaken under the basis of ***informed, documented consent***
- necessary for purposes of ***medical diagnosis, the provision of health and social care treatment, or the management of health and social care systems and services*** or ***necessary for reasons of public health*** in the case of service user health related data;
- necessary for the purposes of ***employment or social security / protection activities***;
- necessary to safeguard and ***protect the vital interests*** of an individual.

The CCG also has lawful basis to process personal data for the following activities due to permissions given to us under ***section 251*** of the NHS Act 2016:

- Commissioning, improving, and planning care services
- Invoice validation
- Risk Stratification

The non-identified data the CCG uses for our commissioning and planning activity is considered to be personal data under the General Data Protection Regulation 2018 (GDPR). The lawful basis for the CCG's processing of this data under the GDPR is:

- 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 9(2)(h) processing is necessary for the purposes of … medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

In the case of disclosure of confidential personal data we will also ensure that we meet the ***Common Law Duty of Confidentiality*** by ensuring that either:

- we have consent from the person, whether explicit or implied (implied consent is where the person could reasonable expect their data to be used in this way and has not objected);
- that this authorised by law or legal proceedings;
- that there is an overriding substantial public interest (for example in case of infectious diseases where the public is at risk).

To ensure that we adequately inform you about the way in which we use personal data, we supplement the information included within this notice with further

information (including the lawful basis applicable) within the following service / activity specific notices which are available from the CCG on request:

- Commissioning
- Delegated Primary Care Commissioning
- Contracting and Finance
- Governance and Administration
- Employment
- Business Intelligence
- Business Intelligence - Services provided for other CCGs
- Surrey CCGs Collaborative Working
- Carers
- Care Homes
- Communications and Engagement
- Continuing Healthcare – Adults
- Continuing Healthcare – Children
- Emergency Preparedness, Resilience and Response and Business Continuity
- Emergency Preparedness, Resilience and Response - Services provided for other CCGs
- Individual Funding Requests
- Quality Monitoring
- Safeguarding – Adults & Children
- Referral Support Service
- Risk Stratification
- Population Health Management
- Surrey Care Record
- Medicines Management – Services provided by CCGs
- Medicines Management – Services provided for GP Practices
- Information Governance
- Learning Disabilities
- Adult Mental Health

The CCG also maintains detailed records of processing and can make this available on request to the DPO.

**Who we may share data with**

We may share your personal data with other organisations and these include:

- CCGs within the Surrey CCG Collaborative, and those in other areas;
- Organisation that we have asked to process this information on our behalf and which include:
    - Commissioning Support Units – NEL CSU and NHS South, Central and West CSU;

    - Providers of employment related services including You HR, our Payroll Provider, and our Occupational Health service provider;
    - Our Auditors (RSM and TIAA);
    - Information, Communication Technology (ICT) system providers;
    - Docobo and Sollis, who undertake risk stratification on behalf of the CCG;
    - Optum Health Solutions UK Limited and Edge Health Limited who provide data analytics and support with population health management activity undertaken within the CCG area;
- Organisations that have a legal right to obtain this from us (such as the NHS Counter Fraud Authority, Police and certain Government Departments).

These organisations are Data Processors of your information and the CCG ensures that they use it only as instructed by us and in accordance with this notice. Our Data Processors may transfer your data outside of the UK or Europe - where this is done we ensure that there is adequate protection in place.

**Your information related rights**

Under data protection legislation everyone has rights regarding how their information can be used and the CCG is committed to ensuring that we and our authorised data processors meet these – please see below for further information:

Under data protection legislation and the NHS Constitution you have the right to be ***informed***, which will meet via this and related notices, and to ***opt-out*** of having your data used for specific purposes.

- You can choose whether your confidential patient information is used for research and planning. To find out more about the NHS National Data Opt-Out programme visit nhs.uk/your-nhs-data-matters.
- You can also tell your GP practice if you do not want your confidential patient information held in your GP medical record to be used for purposes other than your individual care. This is commonly called a Type 1 Opt Out'. This opt-out request can only be recorded by your GP practice.

If you are user of a healthcare related service provided by a CCG you can opt-out by contacting us by email, telephone, or post. We will explain what impact this may have on our ability to provide you with this service.

If you are receiving email communications from us (and we do not require that you receive these for contractual or legal reasons) you will be able to opt-out of receiving further emails by clicking on the unsubscribe link in the email or by contacting us by email, telephone, or post. We immediately remove your details from our mailing list and you will no longer receive these emails from us.

You should also contact us by contacting us by email, telephone, or post if you wish to opt-out and we process your data for other purposes. We will confirm whether we are able to respect this right and provide an explanation if we are not able to do this.

You have the right to ***object*** about the way in which we use your information and to ask us to stop using it in this way. You can do this by contacting us by email, telephone, or post.

- **Service Users** - If you no longer want us to use your information and we no longer require this to supply you with services or to meet our regulatory or legal duties, we will stop using your data.
- **Individuals undertaking work for the CCG** - If we hold your data for employment, governance or administration related purposes, and we no longer require this to meet our contractual, regulatory or legal duties, we will stop using your data if you want us to do this unless we can demonstrate that need to continue process this to meet our legitimate interests.

You have the right to ***erasure*** and to request that we delete your information and we will do this if we no longer require it for the purpose it was provided or to meet a contractual, regulatory or legal duty. Please note that this right does not apply to health data. Please contact us by email, telephone, or post if you want us to delete your data.

You have the right to ***access*** a copy of the information we hold about you by requesting this in writing and we will provide you with a copy of this free or charge and within one calendar month of your valid request – please contact us by email, telephone, or post.

You have the right to have your information ***corrected*** if it is not accurate. Please let us know if you think the information we hold about you is not correct by contacting us by email, telephone, or post and we will update this;

If consent is the legal basis for us to process your information you have the right to ***withdraw consent*** at any time by contacting us by email, telephone, or post.

If you are receiving marketing related email communications from us you will be able to withdraw your consent to receiving the emails by clicking on the unsubscribe link in the email or by contacting us by email, telephone, or post. We immediately remove your details from our mailing list and you will no longer receive these emails from us.

If you are user of a healthcare related service provided by a CCG you can withdraw consent by contacting us by email, telephone, or post. We will explain what impact this may have on our ability to provide you with this service.

If consent is the legal basis for us to process your information and this is held in an electronic format you may also have the right to ***portability*** and to request that this

data be quickly and securely transferred to another similar computer system. Please contact us by email, telephone, or post if you wish to discuss this right.

The CCG does not undertake any ***automated individual decision-making*** (e.g. making a decision solely by automated means without any human involvement). We do however carry out some automated processing to support our commissioning activity and the relevant lawful basis under this is section 6(1)(e) 'official authority' and 9(2)(h) 'processing is necessary for health purposes'. You can object to this processing by contacting us by email, telephone, or post.

**What happens if you change your mind**

You can change your mind about the following at any time and as many times as you like:

- Whether you give your consent for us to process your information;
- Whether you would like to submit an objection or opt-out;
- To withdraw your consent for your information to be used.

If you wish to change your mind please contact us by email, telephone, or post. If this will have an impact on the services we can provide or your care, we will explain this to you before asking you to make your decision.

**The CCG's Data Protection Officer (DPO)**

Under data protection legislation the CCG is required to have a Data Protection Officer (DPO) and it is their role to:

- Inform and advise the organisation and its employees about their obligations to comply with applicable data protection legislation;
- Support and monitor compliance with applicable data protection legislation;
- Be the first point of contact for individuals whose data is being processed.

The CCG's Data Protection Office is Daniel Lo Russo and you can contact them by:

- By Email
- Telephone on 07917 093042

Further information regarding the role of the DPO can be found at link.

**Other people with related responsibilities**

In addition to the DPO, the CCG has in place the following people with related responsibilities:

- Matthew Tait, the ***ICS Chief Officer*** for Surrey Heartlands CCG is accountable for ensuring that the organisation complies with data protection legislation.
- Elaine Newton, ICS Executive Director for Corporate Affairs and Governance is the CCG's ***Senior Information Risk Owner*** (SIRO). They have delegated responsibility (from the ICS Chief Officer) for ensuring the organisation complies with data protection legislation. The SIRO ensures that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.
- The ***Caldicott Guardian*** is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations must have a Caldicott Guardian. Details of the CCG's Caldicott Guardian are available via the public register at link.
- Members of the ***Information Governance Team*** support the above roles in discharging their data related responsibilities

**How we keep information secure**

The CCG ensures that we keep your information (including personal data) secure and handles this in accordance with the 10 Data Security Standards arising from the National Data Guardian's review; which are based around the following areas:

- ***People*** - ensure individuals undertaking work for the organisation are equipped to handle information respectfully and safely, according to the Caldicott Principles;
- ***Processes*** - ensure the organisation proactively prevents data security breaches and responds appropriately to any incidents or near misses;
- ***Technology*** - ensure technology used is secure and kept up-to-date.

We demonstrate our compliance with the Data Security Standards via our annual NHS Data Security and Protection Toolkit submission.

Where our processing of personal data may potentially have significant negative impact on people we follow a privacy by design and default approach and will undertake a detailed Data Protection Impact Assessment to ensure that data protection and confidentiality related risks are identified and suitably mitigated.

**How long we keep information for**

The CCG holds records containing personal data for a limited amount of time and then securely destroys these when they are no longer required. The CCG will ensure that records are held in accordance with the guidance and retention schedules included within the 2016 Records Management Code of Practice for Health and Social Care. Please see our Records Management Policy for further information.

## How to complain

If you wish to complain about the way we use your information we would ask that you initially raise this to us – please see our website for further information on how to do this.

However you are entitled to also contact the Information Commissioner's Office (ICO) if you have concerns about the way your information has been used and you can find their contact them by:

- Visiting their website: www.ico.org.uk
- Telephoning them on 0303 123 1113

## Links to associated guidance

For further associated guidance please see:

- The Information Commissioner's (ICO) Office website which provides independent advice about data protection, privacy and data sharing
- NHSX which provides guidance for health and social care organisations
- The NHS Constitution which includes pledges regarding how information will be used
- The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what controls patients can have over this

## Changes

We will review the information contained within this notice regularly and update it as required. We therefore recommend that you check this webpage regularly to remain informed about the way in which we use your data.

This version was last updated by the DPO on the 27/04/2020.