

FAIR PROCESSING NOTICE

How we use information about you

Who we are:

Castle Point and Rochford Clinical Commissioning Group (CCG) has various roles and responsibilities, but a major part of our work involves making sure that:

- Contracts are in place with local health service providers;
- routine and emergency NHS services are available to patients;
- those services provide high quality care and value for money; and
- paying those services for the care and treatment they have provided.

This is called “commissioning”. See our website for further information about who we are and what we do <http://castlepointandrochfordccg.nhs.uk/>

Accurate, timely and relevant information is essential for our work to help us to design and plan current and future health and care services, evidence and review our decisions and manage budgets.

Our Commitment to Data Privacy and Confidentiality Issues

We are committed at all times to protecting your privacy and will only use information ethically and lawfully in accordance with the General Data Protection Regulations, the Data Protection Act 2018, the Human Rights Act 1998 and the common law duty of confidentiality. The various laws and rules about using and sharing confidential information, with which the CCG will comply, are available in [guide to confidentiality in health and social care](#) which is published on the NHS Digital website.

Castle Point and Rochford CCG is a Data Controller under the terms of the GDPR/DPA 2018 we are legally responsible for ensuring that whenever we collect, use, hold, obtain, record or

share personal confidential data about you, we do it in compliance with GDPR/DPA 2018 Article 5 – Principles Relating to Processing of Personal Data.

All data controllers must register with the [Information Commissioner's Office \(ICO\)](#). Our ICO Data Protection Register number is **ZA007607** 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.

All identifiable 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 authorised staff are able to see information that identifies you. A limited number of authorised staff have access to information that identifies you, but only where it is appropriate to their role and strictly on a need-to-know basis. All health and social care organisations are required to provide annual evidence of compliance with applicable laws, regulations and standards through the Data Security and Protection Toolkit. This shows our current level of compliance as 'Satisfactory' and provides assurance to you on how we protect your information.

All of our staff, contractors and committee members receive 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. All staff are trained to ensure they understand how to recognise and report an incident and the organisation has procedures for investigating, managing and learning lessons from any incidents that occur.

We will only retain information in accordance with the schedules set out in the Records Management Code of Practice for Health and Social Care 2016. The CCG's Records Management Policies include guidance around the secure destruction of information in line with the Code of Practice.

The CCG has a Caldicott Guardian, who is a senior person responsible for protecting the confidentiality of a patient information and enabling appropriate information-sharing. Each NHS organisation is required to have a Caldicott Guardian.

The Caldicott Guardian for Castle Point & Rochford CCG is Tricia D'Orsi, please see the Contact Us section below for contact details.

The GDPR requires an organisation to appoint a data protection officer (DPO) if they are a public authority or body, or if you carry out certain types of processing activities.

DPOs assist organisations to monitor internal compliance, inform and advise on data protection obligations, and act as a contact point for data subjects and the supervisory authority. The DPO for Castle Point and Rochford CCG is Jane Marley.

How the CCG uses your information

There may be times when we need to hold and use certain information about you, for example:

- if we are involved in helping you to resolve a complaint with your GP or other NHS service provider;
- if we fund specialised treatment for you for a particular health condition that is not covered in our local contracts;
- if you are a member of our patient participation group, or have asked us to keep you up to date about our work and involved in our engagement and public consultations,

The information we hold about you personally will therefore be with your knowledge and consent.

There may be times when we need to hold and use certain information for purposes such as:

- determining the general health needs of the population
- ensuring that our services meet future patient needs
- teaching and training healthcare professionals
- investigating complaints, legal claims, etc.
- conducting health research and development.
- preparing statistics on NHS performance
- auditing NHS accounts and service
- paying your health care provider

If you do have any concerns about us holding your personal information, then please tell us and we can explain the way this may affect our ability to help and discuss alternative arrangements available to you.

Legal obligations to collect and use information

In the circumstances where we are required to use personal identifiable information we will only do this if:

- The information is necessary for your direct healthcare, or
- We have received explicit consent from you to use your information for a specific purpose, or
 - There is an overriding public interest in using the information:
 - in order to safeguard an individual,
 - to prevent a serious crime
 - in the case of Public Health or other emergencies, to protect the health and safety of others, or
- There is a legal requirement that allows or compels us to use or provide information (e.g. a formal court order or legislation), or
- We have permission from the Secretary of State for Health to use certain confidential patient identifiable information when it is necessary for our work.

Risk stratification

Risk stratification is a process GPs use to help them to identify and support patients with long-term conditions and to help prevent un-planned hospital admissions or reduce the risk of certain diseases developing such as type 2 diabetes. This is called risk stratification for case-finding.

The CCG also uses risk stratified data to understand the health needs of the local population in order to plan and commission the right services. This is called risk stratification for commissioning.

Risk stratification tools use historic information about patients, such as age, gender, diagnoses and patterns of hospital attendance and admission collected by NHS Digital from NHS hospitals and community care services. This is linked to data collected in GP practices and analysed to produce a risk score.

There is currently s251 support in place for the CCG to be able to receive data with the NHS Number as an identifier from both NHS Digital and your GP Practice to enable this work to take place. The Data is sent directly into a risk stratification tool from NHS Digital /GP Practices to enable the data to be linked and processed as described above. Once the data is within the tool CCG staff only have access to anonymised or aggregated data.

GPs are able to identify individual patients from the risk stratified data when it is necessary discuss the outcome and consider preventative care.

Type of Information Used

Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS.

Information put into the risk stratification tools used by the CCG,

- Age
- Gender
- GP Practice and Hospital attendances and admissions
- Medications prescribed
- Medical conditions (in code form) and other things that affect your health.

Legal Basis

Statutory requirement for NHS Digital to collect identifiable information.

A Section 251 approval (CAG 2-03(a)/2013) from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets.

There is no requirement for a legal basis for use of the aggregated information which is available to the CCG as this does not identify individuals.

Data Processing Activities

The CCG processes this data internally. Data is also processed by Arden & GEM Commissioning Support Unit and Prescribing Services Ltd on behalf of the CCG.

Opt out details

Your GP practice can apply a code which will stop your identifiable information being used for this purpose.

Invoice Validation

Where we pay for care, particularly where different providers are caring for the same person, we may ask for evidence before paying, or we may commission a service where the payment is all or partly based on the providers ensuring the service user has a healthy outcome. We need to ensure that we are paying the right amount of money for the right services to the right people.

These invoices are validated within a special secure area known as a Controlled Environment for Finance (CEff) to ensure that the right amount of money is paid, by the right organisation, for the treatment provided.

A small amount of information that could identify an individual is used within this secure area (such as NHS number or date of birth and postcode). The process followed ensures that only the minimum amount of information about individuals is used by a very limited number of people. The process is designed to protect confidentiality.

Organisations that provide treatment submit their invoices to the CCG for payment. The secure area (Controlled Environment for Finance, within the CCG) receives additional information, including the NHS Number, or occasionally the date of birth and postcode, from the organisation that provided treatment.

Our Providers send information into our secure area, which includes the NHS number and details of the treatment received. The information is then validated ensuring that any discrepancies are investigated and resolved between the Controlled Environment for Finance and the organisation that submitted the invoices. The invoices will be paid when the validation is completed.

Type of Information Used

Identifiable – (name, DOB, GP, NHS number) within the Controlled Environment for Finance, for invoice validation.

Pseudonymised, anonymised or aggregated - within the CCG, for commissioning purposes such as financial planning, management and contract monitoring.

Legal Basis

A Section 251 approval from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority enables the CCG to process identifiable information without consent for the purposes of invoice validation within a Controlled Environment for Finance – CAG 7-07(a)(b)(c)/2013.

Data Processing Activities

This data is processed in house by Castle Point and Rochford CCG. Only authorised staff are able to access this information.

Opt out details

Type 2 opt-out applies. Additionally, your GP practice can apply a code which will stop your identifiable information being used for this purpose.

Additional information is also available from the NHS England website:

<https://www.england.nhs.uk/ourwork/tsd/ig/in-val/invoice-validation-faqs/>

Commissioning

Hospitals and community setting organisations that provide NHS-funded care must by law submit certain information to NHS Digital about services provided to you and the population we serve. This information is known as commissioning datasets. The CCG obtains these datasets from NHS Digital which relate to patients registered with our GP practices. This enables us to plan, design, purchase and pay for the best possible care available for you.

The datasets we receive from NHS Digital have been linked and are in a format that does not directly identify you. Information such as your age, ethnicity and gender as well as coded information about any clinic or accident and emergency attendances, hospital admissions and treatment will be included.

We also receive similar information from the GP Practices within our CCG membership that also does not identify you.

We use these datasets for a number of purposes such as:

- Performance managing contracts;
- Reviewing the care delivered by providers to ensure service users are receiving quality and cost effective care;
- To prepare statistics on NHS performance to understand health needs and support service re-design, modernisation and improvement;
- To help us plan future services to ensure they continue to meet our local population needs;
- To reconcile claims for payments for services received in your GP Practice;
- To audit NHS accounts and services;

Within Essex, the 7 Clinical Commissioning Groups work collaboratively to assess the need for services, and to work together in procuring, negotiating and managing contracts with Hospitals, Mental Health Providers and Community Health Providers. This collaboration is known locally as a Host and Associate Agreement and requires the Host CCG to receive Pseudonymised data (see definitions further on in this document). The information that is shared between the CCGs is governed by a written agreement and a commitment that we will not re-identify it.

The specific terms and conditions and security controls that we are obliged to follow when using those commissioning datasets can also be found on the NHS Digital website. More information about how this data is collected and used by NHS Digital is available on their website <http://www.hscic.gov.uk/patientconf>

Type of Information Used

Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS.

Legal Basis

Statutory requirement for NHS Digital to collect identifiable information.

A Section 251 approval from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the use of pseudonymised information about patients included in the datasets, by the organisations who submitted the information.

There is no requirement for a legal basis for use of the aggregated information which is available to the CCG as this does not identify individuals.

Data Processing Activities

Castle Point and Rochford CCG processes this data internally. Data is also processed by Arden and Greater East Midlands (AGEM) Commissioning Support Unit on behalf of the CCG.

Opt out details

Type 1 and Type 2 opt-outs apply. Additionally, your GP practice can apply a code which will stop your identifiable information being used for this purpose.

Sharing 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 statistical information with them for the purpose of improving local services, for example understanding how health conditions spread across our local area compared against other areas.

In order to perform our commissioning functions, information may be shared between various organisations including: acute and mental health hospitals, GP practices, community services, other CCGs, commissioning support units (CSU), ambulance services, local councils (social services and public health) and voluntary sector and other health organisations.

The law provides some NHS bodies, particularly NHS Digital (formerly the Health and Social Care Information Centre) ways of collecting and using patient data that cannot identify a person. This information helps commissioners to design and procure the combination of services that best suit the population they serve.

We may also share information with NHS England and NHS Digital. If you do not want your information to be used for purposes beyond providing your care you can choose to opt-out. If you wish to do so, please inform your GP practice who will advise you of how to opt out. You can opt out of your data being used for some purposes. You can withdraw your opt-out choice at any time by informing your GP Practice. More information is available on [NHS Digital Your personal information choices](#) and in the section 'Your Rights' below.

NHS Digital takes the responsibility for looking after care information very seriously. Please follow links on how NHS Digital look after information for more detailed documentation.

NHS England recognises the importance of protecting personal and confidential information in all that they do, direct or commission and takes care to meet its legal duties. Follow the links on the [How NHS England uses your information page](#) for more details.

Data may be de-identified and linked 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.

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 GP data with other data such as secondary uses service (SUS) data (hospital inpatient, outpatient and A&E data). In some cases there may also be a need to link local datasets which could include a range of acute-based (hospital) services such as radiology, physiotherapy, audiology etc, as well as mental health and community-based services such as Improving Access to Psychological Therapies (IAPT), district nursing, podiatry etc. When carrying out this analysis, the linkage of these datasets is always done using a unique identifier that does not reveal a person's identity as the CCG does not have any access to patient identifiable data for this purpose.

We may also contract with other organisations to process data. These organisations are known as data processors. 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. Currently, the external data processors we work with are listed below:

Arden & Greater East Midlands (AGEM) Commissioning Support Unit (CSU) which includes Data Services for Commissioners Regional Office (DSCRO), who provide appropriate data for Secondary Use Services (SUS).

AGEM are approved by NHS England as a Data Services for Commissioning Regional Office (DSCRO). They provide a secure and compliant data processing function of health and social care data sets. This type of processing is to support commissioning and planning. The output data from this process will be anonymised or pseudonymised. The CCG does not receive any personal identifiable information from this service.

AGEM CSU also provide IT services for the CCG, This includes holding and processing data including patient information on our behalf, and providing human resources services for our staff.

Your rights

You have certain legal rights, including a right to have your information processed fairly and lawfully and in a transparent manner, and a right to access any personal information we hold

about you. You have the right to privacy and to expect the NHS to keep your information confidential and secure.

If we do hold identifiable information about you, you can ask us to correct any mistakes by contacting us at the address detailed in the Contact Us section below.

You have the right to ask us to stop processing information about you where we are not required to do so by law – although we will first need to explain how this may affect the care you receive.

In some instances, you are allowed to request that your confidential information is not used beyond your own care and treatment and to have your objections considered. If your wishes cannot be followed, you will be told the reason (including the legal basis) for that decision.

If you wish to exercise your right to opt-out, or to speak to somebody to understand the impact this may have, if any, please contact us.

If you wish to know what personal information the CCG holds about you, or to request access to that information, then please contact us.

To protect your confidentiality, you will have to provide proof of who you are.

All information held by the CCG is governed by the CCG's information lifecycle management policy and is held, retained and destroyed in line with the Records Management Code of Practice for Health and Social Care (see link under further information below).

Contact us

If you have any questions, complaints or concerns about how we use your information, please contact us at:

NHS Castle Point and Rochford Clinical Commissioning Group
Pearl House
12 Castle Road
Rayleigh
Essex
SS6 7QF

Tel: 01268 464508

Email: cpr.ccg@nhs.net

Caldicott Guardian – Tricia D'Orsi – 01268 464508

Data Protection Officer – Jane Marley – 01268 594350

dpo.cprccg@nhs.net

Definitions

Below are some key definitions of terms used within this notice:

Personal Data – Data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of the CCG (for example, name, address, date of birth, NHS Number)

Sensitive Personal Data (in the context of the NHS) – Data consisting of information as to an individual's physical or mental health or condition

Pseudonymised Data – Pseudonymisation is a technical process that replaces identifiable information such as a 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 Data – Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place.

Aggregated Data – the consolidation of data relating to multiple individuals, and therefore the data cannot be traced back to a specific individual.

Anonymised Patient Level Data – Activity level data which has had identifiers removed so as to render it anonymous.

Primary Care Data – primary care refers to the work of health professionals who act as a first point of contact for patients such as GP's and pharmacists, primary care data is therefore data collected within GP Practices, dental practices, community pharmacies and high street optometrists.

Secondary Care Data – secondary care is the health care provided by specialists who generally do not have first contact with patients, it includes hospital care, community care and mental health care, secondary care data is therefore data collected by hospital, mental health and community services.