

FAIR PROCESSING NOTICE

NHS County Durham Clinical Commissioning Group

Sedgefield Community Hospital
Salters Lane
Sedgefield
County Durham
TS21 3EE
Telephone: 0191 371 3222

The Lavender Centre
Pelton
Chester-le-Street
County Durham
DH2 1HS**Telephone:** 0191 389 8600

Transfer of information

Information that has been held previously by NHS Durham Dales, Easington and Sedgefield CCG and NHS North Durham CCG is transferring to the new NHS County Durham CCG on 1 April 2020. The new CCG will become the new data controller. Any questions about the use of data (including patient data) by the new CCG should be directed to cdccg.enquiries@nhs.net.

Our Clinical Commissioning Group (CCG) holds some information about you. This notice is to inform you of the type of information (including personal information) that the CCG holds, how that information is used, with whom we may share that information and how we keep it secure and confidential.

What we do

Our CCG is responsible for planning, buying and monitoring (also known as commissioning) Primary Care and Secondary Care services. Secondary Care services are usually (but not always) delivered in a hospital or clinic with the initial referral being received from Primary Care.

We commission these health services from hospitals and GP practices for our local population to ensure the highest quality of healthcare. We also have a performance monitoring role of these services, which includes responding to any concerns from our patients on services offered. Further details about what we do are on our web site. To help us to model and plan services to best meet your future healthcare needs, the CCG needs to understand the health, social and general wellbeing issues that people are facing today. The only way we can achieve this is by using the information that your GP, your clinician or your social worker enter into your care record.

How we use your information

Our CCG holds some information about you and this document outlines how that information is used, with whom we may share that information, how we keep it secure (confidential) and what your rights are in relation to this. The [NHS Care Record Guarantee for England](#) sets out the rules that govern how patient information is used in the NHS and what control patients can have over this.

The [NHS 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.

We keep a Register of all our information processing activities, including those involving the use personal information. This records lots of metadata including where we get the information from, with whom we share it, the legal basis allowing us to process personal data and the security arrangements in place.

Our legal basis for processing personal data

The CCG is a public body established by the NHS Act 2006 as amended by the Health and Social Care Act 2012. As such our business is based upon statutory powers which underpin the legal bases that apply for the purposes of the GDPR. The legal bases for the majority of our processing is:

Article 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.

For entering into and managing contracts with the individuals concerned, for example our employees the legal basis is:

Article 6(1)(b) – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Where we have a specific legal obligation that requires the processing of personal data, the legal basis is:

Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.

Where we process special categories data, for example data concerning including health, racial or ethnic origin, or sexual orientation, we need to meet an additional condition in the GDPR. Where we are processing special categories personal data for purposes related to the commissioning and provision of health services the condition is:

Article 9(2)(h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

OFFICIAL

Where we process special categories data for employment or safeguarding purposes the condition is:

Article 9(2)(b) – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.

We may also process personal data for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or for the purpose of establishing, exercising or defending legal rights.

Where we process personal data for these purposes, the legal basis for doing so is:

Article 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; or

Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject; or

Article 6(1)(f) – processing is necessary for the purposes of legitimate interests pursued by the controller.

Where we process special categories of personal data for these purposes, the legal basis for doing so is:

Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; or

Article 9(2)(g) – processing is necessary for reasons of substantial public interest.

What kind of information do we use?

We use the following types of information/data:

- **Personal Confidential Information** - this term describes personal information or data about identified or identifiable individuals, which should be kept private or secret. For the purposes of this notice 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive', as defined in the Data Protection Act.
- **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** - Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

What do we use anonymised information for?

We use anonymised information to plan healthcare 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 will 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

What do we use your personal and confidential/sensitive information for?

For the purposes listed above, we will only use anonymised data which means that individuals can not be identified. We can only use any information that may identify you (known as personal information) in accordance with data protection legislation and other laws such as the [Health and Social Care Act 2012](#).

Therefore, as a commissioning organisation we do not routinely hold medical records or confidential patient data. There are some limited exceptions where we may hold and use personal information about you; for example the CCG is required by law to perform certain services that involve the processing of sensitive personal information. The areas where we regularly use sensitive personal information include:

- a process where you or your GP can request special treatments that is not routinely funded by the NHS, which are known as [Individual Funding Requests](#)
- assessments for [continuing healthcare](#) (a package of care for those with complex medical needs) and appeals
- responding to your [queries, compliments, complaints or concerns](#) - such requests are processed by North of England Commissioning Support Unit on our behalf
- assessment and evaluation of [safeguarding](#) concerns – we have official authority to do this and to safeguard the rights and interests of individuals
- where there is a provision permitting the use of sensitive personal information under specific conditions, for example to:
 - understand the local population needs and plan for future requirements, which is known as “Risk Stratification for commissioning” – this is explained further later in this document
 - ensure that the CCG is billed accurately for the treatment of its patients, which is known as “invoice validation” – this is explained further later in this document
 - monitor access to services, waiting times and particular aspects of care, for which the CCG is considered to be an “accredited safe haven”.

Sensitive personal information may also be used in the following cases:

- The information is necessary for your direct healthcare
- To respond to patients, carers or Member of Parliament communication
- We have received consent from individuals to be able to use their information for a specific purpose.
- There is an over-riding 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).

OFFICIAL

- For the health and safety of others, for example to report an infectious disease such as meningitis or measles.
- We have special permission for health and research purposes (granted by the Health Research Authority).
- We have special permission called a 'section 251 agreement' (Section 60 of the Health and Social Care Act 2001 as re-enacted by Section 251 of the NHS Act 2006) which allows the Secretary of State for Health to make regulations to set aside the common law duty of confidentiality for defined medical purposes. An example of where this is used is in risk stratification. Further information can be found on the Health Research Authority's [web site](#)

The following list includes examples of where we collect and use personal information. Please click on each of the following examples for information on the purpose, the type of information used, the legal basis identified for the collection and use of the information, how we collect and use the information required, any third parties we may share the information with and your rights regarding the use of the information including, where relevant, your right to opt out.

- [Commissioning](#)
- [Risk Stratification](#)
- [Invoice Validation](#)
- [Complaints](#)
- [Individual Funding Requests \(IFR\)](#)
- [Continuing Healthcare](#)
- [Personal Health Budgets \(PHBs\)](#)
- [Safeguarding](#)
- [Patient and Public Involvement](#)
- [Serious Incident reports](#)
- [Freedom of Information requests](#)
- [Medicines Management](#)
- [Care and Treatment Reviews](#)
- [Referral Support Services](#)
- [Film and Promotional Materials](#)
- [Information for Job Applicants](#)
- [Human Resources](#)
- [Declarations of Interest](#)
- [National Fraud Initiative](#)

Risk stratification

Risk stratification is targeted healthcare intervention which applies computer-based algorithms or calculations to identify those patients registered with the GP practice who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition. Currently this is carried out via a section 251 agreement. We use the services of a health partner, North of England Commissioning Support Unit (NECS) to do this. Minimal identifiers are used for this purpose, such as NHS number, post code, date of birth; data may be linked with other data for the purpose of risk stratification. Further information can be found on NHS England's web site [here](#)

Opting Out - 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. Further information about risk stratification is available from: <https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/>

National Data Opt Out is available – this is explained further under the section entitled Your Right to Opt Out.

Do you share my 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 we may share with local authorities in helping to understand how health conditions spread across our local area compared against other areas or with social care organisations to help better co-ordination of health and social care services. Your health data may at times be linked with data from social care services allowing commissioners to understand your complete health and care needs. This is vital to support the national ambition of seamless services between the NHS and social care. Where this linkage takes place it is done using pseudonymised data such that those using the data have no means of identifying individuals.

We do not routinely share identifiable personal data with organisations not listed within this notice but we may need to share with other organisations for specific purposes on a case by case basis, for example Individual Funding Requests but this is done with patient consent. The law provides some NHS bodies, particularly the Health and Social Care Information Centre (NHS Digital), 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.

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 and they will mark your choice in your medical record. 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](#)

NHS Digital takes the responsibility for looking after care information very seriously. Please follow links on [how we look after information](#) for more detailed documentation.

NHS England recognises the importance of protecting personal and confidential information in all that it does, directs or commissions, and takes care to meet its legal duties. Follow the links on the [How we use your information](#) page for more details.

Data may be de-identified and linked by these special bodies so that it can be used to improve healthcare 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 (inpatient, outpatient and A&E). In some cases there may also be a need to link local datasets which could include a range of acute-based 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.

OFFICIAL

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 include NHS North of England Commissioning Support Unit, which is based at John Snow House, Durham, DH1 3YG and which has been granted a legal basis for processing data for us and which operates under strict controls to ensure your information is handled lawfully.

We record any instances where we transfer personal information to a third country or international organisation. This is very limited and we check and record the safeguards in place to protect the information to be transferred.

Paying Invoices

The validation of invoices is undertaken within a controlled environment for finance within the North of England CSU (NECS) which is based at John Snow House, Durham, DH1 3YG. This is carried out via a section 251 agreement and is undertaken to ensure that the CCG is paying for treatments relating to its patients only. The dedicated NECS team receives patient level information (minimal identifiers are used for this purpose, such as NHS number, post code, date of birth) direct from the hospital providers and undertakes a number of checks to ensure that the invoice is valid and that it should be paid for by the CCG. The CCG does not receive or see any patient level information relating to these invoices. Further information about invoice validation can be found on NHS England's web site [here](#)

YOUR RIGHTS

Right Of Access To Your Personal Information

We will tell you if we use your personal information, what that information is and why we use it. We will also tell you where we obtained the information from and with whom we share your information. Under this right we also have to tell you how long we intend to keep your information for.

The CCG does not directly provide health care services and therefore does not hold personal healthcare records. If you wish to have sight of, or obtain copies of your own personal health care records you will need to apply to your GP Practice, the hospital or organisation which provided your health care.

You are entitled to obtain a copy of the personal information held about you by the CCG. You can view this or request copies of the records by making a **subject access request**. Any request to access or obtain a copy of this information will be considered in line with the data protection legislation. This is generally free of charge unless your request is very complicated and/or unreasonably excessive; if you require further copies of information already provided to you we may charge a reasonable administrative fee. If you want to access your data you can contact us using the contact details at the top of this notice. Under special circumstances, some information may be withheld.

Right To Rectification

This right allows you to ask for any information you believe to be inaccurate or incomplete to be corrected and completed. We are allowed one month from the date of your request in which to perform any such corrections or add supplementary statements.

We will communicate any rectification of information to anyone to whom it has been disclosed unless this is not possible or involves disproportionate effort. We will tell you who those recipients are if you ask us.

Right To Erasure

This right is also commonly referred to as the 'right to be forgotten'. You can request that your information be erased, subject to certain exemptions, if it is no longer needed by us for the original purpose we said we would use it for or if you decide to withdraw your consent or if you object to the use of your information. If it transpires that the information was unlawfully used or is found to infringe the law you can ask for it to be erased. We will erase your information if we have a legal obligation to do so. We will communicate any erasure of information to anyone to whom it has been disclosed unless this is not possible or involves disproportionate effort. We will tell you who those recipients are if you ask us.

Right To Restriction Of Processing

Restriction means marking information with the aim of limiting its processing in the future. Under this right you can request we restrict information processing for a period of time if you think the information is inaccurate, while we check its accuracy. If the information is found to have been used unlawfully you can ask for it to be restricted instead of being erased. If we no longer need to keep the information but you need us to keep it in connection with a legal claim you are involved with you can ask us to restrict it. You can also ask us to restrict processing if you have previously objected to us processing it whilst we check whether our legitimate reasons for processing it outweigh your right. Once processing has been restricted we can start to use the information again only if you have consented to this or where it is in connection with a legal claim or if it is to protect the rights of another person or there is a strong public interest. We will tell you before any restriction we have put in place is lifted. We will communicate any restriction of processing to anyone to whom it has been disclosed unless this is not possible or involves disproportionate effort. We will tell you who those recipients are if you ask us.

Right To Data Portability

The purpose of this new right is to give a person more control over their personal information. Data Portability means you have the right to receive a copy of personal information which you have given us in a structured, commonly-used, machine-readable format and to have it transferred directly to another 'controller' where technically possible. This right only applies to information which is processed by automated means and where you have given consent to the processing or where processing is necessary for the performance of a contract. It does not apply if the processing is needed to comply with a legal obligation, our official duties or is for a task carried out in the public interest. It is therefore unlikely to apply to any of the processing carried out by the CCG.

Right To Object

You can object to the processing of your personal information if the processing activity is necessary for the performance of a task carried out in connection with our lawful, official duties or those of a third party, or a task carried out in the public interest. We could refuse to comply with a request only where we could show that there was an overriding legal reason or if we need to process the information in relation to a legal claim.

You also have a separate right to object to processing if it is for direct marketing purposes. We do not use your information in this way but if we did we would tell you about it. This right also includes a specific right to object to research uses except where this is done in the public interest.

Automated Decision-Making, Including Profiling

Profiling means any form of automated processing (i.e. processed by a computer and not a human being) of personal information used to analyse, evaluate or predict things about someone; this can include things like someone's health, personal preferences, interests, economic situation, reliability, performance at work behaviour, location or movements. Under this right you can ask not to be subject to a decision made solely by automated means, including any profiling, which affects you in a legal way or has a similar significant effect. Automated decision-making and profiling is not allowed if it involves certain types of information; these 'special categories' of information are deemed to carry more sensitivity therefore we cannot use your health information for automated decision-making or profiling unless we have your explicit consent or there is substantial public interest allowing us to do so. We currently do not carry out any automated decision-making, including profiling.

Consent

Where processing is based on consent you have the right to withdraw consent to process your personal data

Right to Complain to the Information Commissioner's Office

You have right to complain to the Information Commissioner if you think any processing of your personal data infringes data protection legislation.

If you wish to exercise your rights or to speak to somebody to understand more, please contact us using the contact details at the top of this notice.

Data Protection Officer (DPO)

As a public authority the CCG must appoint a DPO. The DPO is an essential role in facilitating 'accountability' and the organisation's ability to demonstrate compliance with the data protection legislation.

The DPO for the CCG is Liane Cotterill, who can be contacted via email at NECSU.IG@nhs.net

How do we keep your information secure and confidential?

We only use information that may identify you in accordance with Data Protection legislation. The legislation requires us to process personal data only if there is a legitimate basis for doing so and that any processing must be fair and lawful.

Within the health sector, we also have to follow the common law duty of confidence, which means that where identifiable information about you has been given in confidence, it should be treated as confidential and only shared for the purpose of providing direct healthcare.

The [NHS Digital Code of Practice on Confidential Information](#) 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 and 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).

OFFICIAL

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

We have a senior person responsible for protecting the confidentiality of patient information and enabling appropriate information sharing. This person is called the Caldicott Guardian. The Caldicott Guardian for the CCG is Mr Ian Davidson, Director of Quality and Safety, who can be contacted using the contact details at the top of this document. We also have a Senior Information Risk Owner (SIRO) who is responsible for owning the CCG's information risk. The SIRO is Nicola Bailey, Chief Operating Officer. They are supported by the Quality, Risk and Innovation Committee which meets regularly to discuss information governance issues.

We are registered with the Information Commissioner's Office (ICO) as a data controller which describes the purposes for which we process personal data. A copy of the registration is available from the [ICO's web site](#) by searching on our CCG name.

How long do you hold information for?

All records held by the CCG will be kept for the duration specified by national guidance from the Department of Health, [The Records Management Code of Practice for Health and Social Care 2016](#). Confidential information is securely destroyed in accordance with this code of practice.

Your right to opt out

The national data opt-out is a new service that allows people to opt out of their confidential patient information being used for research and planning. It was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. 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 has had it automatically converted to a national data opt-out from 25 May 2018 and has received a letter giving them more information and a leaflet explaining the new national data opt-out. If a patient wants to change their choice, they can use the new service to do this. You can find out more from by clicking [here](#)

Patients who have a type 1 opt-out

Some patients will have a type 1 opt-out registered with their GP practice, which prevents their confidential patient information leaving the practice for research and planning purposes. These existing type 1 opt-outs will continue to be respected until 2020, when the Department of Health and Social Care will consult with the National Data Guardian on their removal.

If your wishes cannot be followed, you will be told the reasons (including the legal basis) for that decision. There are certain circumstances where a person is unable to opt out but these are only where the law permits this such as in adult or children's safeguarding situations.

You have a right in law to refuse or withdraw previously granted consent to the use of your personal information. There are possible consequences of not sharing such as the effect this may have on your care and treatment but these will be explained to you to help with making your decision.

If you wish to exercise your right to opt-out, or to speak to somebody to understand what impact this may have, if any, please contact us using the contact details at the top of this document.

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.

What sort of information can I request?

In theory, you can request any information that the CCG holds, that does not fall under an exemption. Information that is covered by Data Protection legislation will be handled under that legislation.

How do I make a request for information?

Your request must be in writing and can be either posted or emailed to the CCG. The service is managed by the Information Governance team at NECS. Details of how to apply can be found on our web site

Where can I obtain further advice?

For independent advice about data protection, privacy, data sharing issues and your rights you can contact the Information Commissioner's Office.

Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Telephone: 0303 123 1113 (local rate) or 01625 545 745
Email: casework@ico.org.uk
Visit the ICO website [here](#)

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. Please contact us using the contact details at the top of this document should you have any such concerns.

We keep our privacy notice under regular review.

APPENDIX A

Details of information used for specific purposes

Commissioning

Data Controller(s)	NHS County Durham CCG
Purpose	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 patient registered with our GP Practices. This enables us to plan, design, purchase and pay for the best possible care available for you.
Type of Information Used	<p>Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS.</p> <p>Identifiable – when disclosed from Primary and Secondary care services to NHS Digital</p> <p>Pseudonymised – the CCG may only receive this information in a pseudonymised format which does not identify individuals.</p>
Legal Basis	<p>Statutory requirement for NHS Digital to collect identifiable information.</p> <p>For use by the CCG:</p> <p>GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller</p> <p>GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p> <p>NHS Digital has a legal basis for passing on patient data under the Health and Social Care Act 2012.</p>
How we collect (the source) and use the information	<p>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.</p> <p>We also receive information from the GP Practices within our CCG that does not identify you.</p> <p>We use these datasets for a number of purposes such as:</p> <p>Performance managing contracts</p> <p>Reviewing the care delivered by providers to ensure service users</p>

OFFICIAL

	<p>are receiving quality and cost effective care</p> <p>To prepare statistics on NHS performance to understand health needs and support service redesign, modernisation and improvement</p> <p>To help us plan future services to ensure they continue to meet our local population needs</p>
Data Processors	<p>The Data Services for Commissioning Regional Office (DSCRO) obtains the identifiable information from the Secondary Uses Service (SUS) at NHS Digital. The DSCRO also receives identifiable information directly from providers They pseudonymise the information and pass it to NECS. NECS run further data quality checks and prepare the data for use by the CCG. The primary care data is collected nationally and passed to NHS Digital who then (via the DSCRO) pass on the Information to NECS/CCG.</p>
Your Rights	<p>If you do not want the NHS to use information about you, collected by your GP then you can opt out by completing an opt-out form and returning it to your GP practice. Details of the national patient opt out can be found here: https://www.nhs.uk/your-nhs-data-matters/</p> <p>With regards to Commissioning under GDPR you have the right :</p> <ul style="list-style-type: none"> To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	<p>The data will be retained for a period of 8 years in accordance with the CCG rules outlined in the Records Management: NHS Code of Practice. Data that supports trend analysis or identification of patterns may be held for longer.</p>
Who we will share the information with (recipients)	<p>This information is not shared outside of the CCG.</p>

Risk Stratification

Data Controller(s)	NHS County Durham CCG
Purpose	Information from health and social care records, using the NHS Number provided via the Secondary Uses Service (SUS) at NHS Digital, is looked at to identify groups of patients who would benefit from some additional help from their GP or care team. This is known as 'Risk Stratification'. The aim is to prevent ill health and possible future hospital stays, rather than wait for you to become sick. You have the right to opt out of your information being shared by NHS Digital; please see the Your Right to Opt Out section below.
Type of information Used	Only de-identified information (NHS number removed) is accessible to the CCG. Only GP Practices within the CCG have access to identifiable information (NHS Number) of their own patients in order to see who may benefit from additional help.
Legal basis	GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller. GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services. A section 251 approval (CAG 7-04(a)/2013) from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the pseudonymised information to be sent to the CCG via NHS Digital in order to help us plan the most appropriate health services for our population.
How we collect (the source) and use the information	Primary Care data extracted from individual GP practices and Secondary Care data (collected nationally via the Secondary Uses Service): Inpatient, Outpatient, Accident and Emergency, Out of Hours, Urgent Care, Community Nursing, Community Mental Health is passed to the Data Services for Commissioners Regional Office (DSCRO) so that the information can be linked (the DSCRO is a department of NHS Digital). This information is passed to NECS who provides the Risk Stratification tool to GP Practices on behalf of the CCG. De-identified information is made available to the CCG to provide a picture of the health and needs of their local population, which enables: priorities to be determined in the management and use of resources; planning services; cover the range of potential questions, and issues they may need to consider, and to support and evidence decisions.
Data Processors	North of England Commissioning Support (NECS)
Your Rights	If you do not want the NHS to use information about you, collected by your GP then you can opt out by completing an opt-out form and returning it to your GP practice. Details of the national patient opt

OFFICIAL

	<p>out can be found here: https://www.nhs.uk/your-nhs-data-matters/</p> <p>With regards to Risk Stratification under GDPR you have the right:</p> <ul style="list-style-type: none">To be informed about the processing of your information (this notice)Of access to the information held about youTo have the information corrected in the event that it is inaccurateTo restrict or stop processingTo object to it being processed or usedNot to be subject automated decision-taking or profilingTo be notified of data breaches
How long we will keep the information	<p>The data will be retained in accordance with the CCG rules outlined in the Records Management: NHS Codes of Practice. Specifically for the Risk tool, the system will hold 3 years of data updated monthly to be used within the tool.</p>
Who we will share the information with (recipients)	<p>This information is not shared outside of the CCG.</p>

Invoice Validation

Data Controller(s)	NHS County Durham CCG
Purpose	<p>Invoice validation is part of the process by which providers of care or services get paid for the work they do.</p> <p>Invoices, with supporting information, are submitted to the CCG for payment, but before payment can be released, the CCG needs to ensure that the activity claimed for each patient is their responsibility. 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. The process followed ensures that only the minimum amount of information about individuals is used by a very limited number of people and is designed to protect confidentiality.</p>
Type of information Used	Identifiable (NHS number, date of birth or postcode) and Special Category (health information)
Legal basis	<p>GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller.</p> <p>GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p> <p>A section 251 approval 7-07(a)(c)/2013 from the Secretary of State, through the Confidentiality Advisory Group of the Health Research Authority, enables the CCG to process identifiable information for the purpose of invoice validation within a Controlled Environment for Finance.</p>
How we collect (the source) and use the information	<p>Organisations that provide treatment submit their invoices to the CCG for payment. The nominated secure area (CEfF) receives additional information, including the NHS Number, or occasionally date of birth and postcode, from the organisation that provided the treatment.</p> <p>NHS Digital sends information into the secure area, including the NHS number and details of the treatment received. The information is then validated ensuring that any discrepancies are investigated and resolved between the CEfF and the organisation that submitted the invoice. The invoices will be paid when the validation is completed.</p> <p>The CCG does not receive any identifiable information for purposes of invoice validation; however we do receive aggregated reports to help us manage our finances.</p>
Data Processors	The Controlled Environment for Finance uses NECS North of England Commissioning Support (NECS) as a Data Processor.
Your Rights	For Invoice Validation Type 2 opt outs are not applied; patients can object however these objections should not be upheld in order to pay for Health and Social care services.

OFFICIAL

	<p>With regards to Invoice Validation under GDPR you have the right:</p> <ul style="list-style-type: none">To be informed about the processing of your information (this notice)Of access to the information held about youTo have the information corrected in the event that it is inaccurateTo object to it being processed or usedNot to be subject automated decision-taking or profilingTo be notified of data breaches
How long we will keep the information	<p>This information will be kept for a period of 8 years. This is in line with the Records Management: NHS Code of Practice for Health and Social Care.</p>
Who we will share the information with (recipients)	<p>This information is not shared outside of the CCG.</p>

Complaints

Data Controller(s)	NHS County Durham CCG
Purpose	<p>Under the NHS Complaints Procedure, individuals have a right to complain to both providers and commissioners about services provided by the NHS.</p> <p>A complaint may relate to a service which the CCG is directly responsible for providing, or it may relate to a service which we have commissioned for the patients who we are responsible for, for example hospital services. The CCG requires this information in order to investigate and help to resolve complaints.</p>
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	<p>GDPR Article 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 &</p> <p>GDPR Article 6(1)(c) ‘processing is necessary for compliance with a legal obligation</p> <p>Under:</p> <p>The Local Authority Social Services and National Health Service Complaints (England) Regulations 2009 For further information please visit: http://www.legislation.gov.uk/ukxi/2009/309/contents/made</p> <p>GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p>
How we collect (the source) and use the information	<p>When the CCG receives a complaint from a person, a complaint file is made up which will normally contain the identity of the complainant, the identity of the patient (where this is a different person) and any other individuals involved, plus details of the complaint, including health information.</p> <p>The CCG will only use the identifiable information we collect to process the complaint and to check the level of service we provide.</p> <p>Where the complainant is not the patient, the CCG will usually need to disclose the complainant’s identity to whoever the complaint is about in order to obtain consent under the Common Law Duty of Confidentiality to proceed with the complaint and for the complainant to correspond with us on behalf of the patient.</p>
Data Processors	The CCG uses NECS North of England Commissioning Support (NECS) as a Data Processor.

OFFICIAL

Your Rights	With regards to Complaints under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing Object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	We will keep information in relation to complaints for a period of 10 years.
Who we will share the information with (recipients)	Where complaints relate to a service we commission, such as hospital care, the complaint will be shared with that organisation. The complainant will be informed where this occurs.

Individual Funding Requests (IFR)

Data Controller(s)	NHS County Durham CCG
Purpose	To fund specific treatment for you for a particular condition that is not covered in our contracts with providers. Individual Funding Requests provide payments required to receive specialist treatment, not routinely provided on the NHS, on a case by case basis.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information) – to make payments Anonymous – to provide reports for analysis of payments made
Legal basis	GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.
How we collect (the source) and use the information	Information required to make payments in relation to funding treatments is provided by you, along with relevant information from primary and secondary care regarding the referral for specialist treatment. The CCG will only use the identifiable information we collect to process the request for funding. This process is carried out with the consent of the patient to satisfy the Common Law Duty of Confidentiality.
Data Processors	<u>North of England Commissioning Support (NECS)</u>
Your Rights	With regards to Individual Funding Requests under GDPR you have the right : To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The organisation has adopted the retention periods for health and non-health records as set out in the Records Management Code of Practice for Health and Social Care 2016. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016. For Individual funding requests this is 6 years after the end of the financial year to which they relate.
Who we will share the information with (recipients)	This information will be shared with NECS, GP's, and health and care organisations involved in delivering or arranging the Individual Funding Request.

Continuing Healthcare

Data Controller(s)	NHS County Durham CCG
Purpose	Where you have asked us to undertake assessments for Continuing Healthcare – a package of care for those with complex needs. We use your information in order to be able to make the appropriate arrangements for assessing your needs. Individual consent will be sought before any information about you is sought from other professionals.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.
How we collect (the source) and use the information	The CHC team will collect, use, share and securely store information from/with the Local Authority (Social Services) and other organisations or individuals that are either directly or indirectly involved in the assessment, decision making process, the arranging of care, the funding and payment of care and appropriate monitoring of and audit of the safety and quality of care. This process is carried out with the consent of the patient to satisfy the Common Law Duty of Confidentiality.
Data Processors	The CCG does not use external data processors for this function.
Your Rights	With regards to Continuing Healthcare under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The CCG will keep this information for a period of 8 years. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016.
Who we will share the information with (recipients)	The Local Authority (Social Services), Care Homes, health and care organisations involved in delivering or arranging the continuing care required.

Personal Health Budgets (PHBs)

Data Controller(s)	NHS County Durham CCG
Purpose	<p>A personal health budget is an amount of money to support someone's health and wellbeing needs, which is planned and agreed between the person, or their representative, and the local clinical commissioning group (CCG) or NHS team.</p> <p>The amount in someone's personal health budget is based upon their personalised care and support plan. This plan helps people to identify their health and wellbeing outcomes, together with their local NHS team, and sets out how the budget will be spent to enable them to reach their goals and keep them healthy and safe.</p>
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	<p>GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller</p> <p>GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p> <p>Relevant legislation: National Health Service (Direct Payments) Regulations 2013</p>
How we collect (the source) and use the information	<p>A personal health budget is based upon a personalised care and support plan. This plan sets out someone's health and wellbeing needs, the outcomes they wish to achieve, the amount of money available and how it will be spent. Once the plan and budget has been agreed, the money in a personal health budget can be managed in three ways, or a combination of these:</p> <p>Notional budget: No money changes hands. The personal health budget holder knows how much money is available for their assessed needs and decides together with the NHS team how to spend that money. The NHS is then responsible for holding the money and arranging the agreed care and support.</p> <p>Third party budget: An organisation independent of both the person and the NHS commissioner (for example an independent user trust or a voluntary organisation) is responsible for and holds the money on the person's behalf. They then work in partnership with the person and their family to ensure the care they arrange and pay for with the budget meets the agreed outcomes in the care plan.</p> <p>Direct payment for healthcare: The personal health budget holder or their representative has the money in a bank account and takes responsibility for purchasing the agreed care and support. Budget holders must show what the money has been spent on. Further guidance is included in the Direct Payments in Healthcare Guidance.</p>

OFFICIAL

	<p>In most cases people will need a separate bank account to receive a personal health budget via a direct payment (there are some exceptions when the money can be paid directly into someone's existing account, for example if it is a one-off payment). The separate account must only be used for purchasing care, but it may also be used for receiving and managing a social care personal budget, if someone has an integrated personal budget.</p> <p>If someone wishes to have a personal health budget but doesn't want to manage it themselves or doesn't have the capacity to manage the budget themselves, it may be possible for someone else to manage the budget on their behalf. This might be a family member, a close friend or representative. Regardless of who is responsible for the budget, every effort must be made to ask the person about their wishes and to keep their best interests in mind.</p> <p>This process is carried out with the consent of the patient to satisfy the Common Law Duty of Confidentiality.</p>
Data Processors	The CCG does not use external data processors for this function.
Your Rights	<p>With regards to Personal Health Budgets under GDPR you have the right:</p> <ul style="list-style-type: none"> To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The CCG will keep this information for a period of 8 years. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016.
Who we will share the information with (recipients)	The Local Authority (Social Services), health and care organisations involved in delivering or arranging the care required. The third party (for example an independent user trust or a voluntary organisation, or payroll/managed account provider) looking after your money where this has been arranged. If someone wishes to have a personal health budget but doesn't want to manage it themselves or doesn't have the capacity to manage the budget themselves, it may be possible for someone else to manage the budget on their behalf (e.g. family member, friend or representative, nominee).

Safeguarding

Data Controller(s)	NHS County Durham CCG
Purpose	The CCG has a legal duty to have arrangements in place for safeguarding both adults and children. In order to carry out this role, the CCGs' Safeguarding Team processes information for safeguarding purposes.
Type of information Used	<p>Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)</p> <p>The information processed for relevant people only, can include; names, date of birth, address, NHS number, relevant and proportionate information concerning their health and care and their racial or ethnic origin where this is relevant. The CCG will only share this personal information where expressly permitted by law, and will not share with any partners who do not have a lawful basis to process the personal information.</p>
Legal basis	<p>GDPR Article 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...'</p> <p>GDPR Article 9(2)(b) 'processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of ...social protection law in so far as it is authorised by Union or Member State law..'</p> <p>The Children Act 1989 & 2004 establishes implied powers for local authorities and relevant partner agencies to share information to safeguard children. Local authorities have a duty to investigate where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm is the subject of an emergency protection order, or is in police protection.</p> <p>The Children Act also requires local authorities 'to safeguard and promote the welfare of children within their area who are in need' and to request help from specified authorities including NHS Trusts and Foundation Trusts, NHS England and CCGs. These are required by the Children Act to comply with such requests. Under the Children Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being.</p> <p>The Criminal Justice Act 2003 provides for the establishment of Multi-Agency Public Protection Arrangements ("MAPPA") in England and Wales. Under this legislation the NHS have a duty to co-operate with MAPPA processes by sharing relevant and proportionate information regarding MAPPA subjects.</p> <p>The Care Act 2014 requires that local authorities must make enquiries, or cause another agency to do so, whenever abuse or neglect are suspected in relation to an adult and the local authority thinks it necessary to enable it to decide what (if any) action is</p>

OFFICIAL

	<p>needed to help and protect the adult.</p> <p>The Care Act 2014 stipulates that partners should ensure that they have the mechanisms in place that enable early identification and assessment of risk through timely information sharing and targeted multi-agency intervention.</p> <p>Decisions on sharing information must be justifiable and proportionate, based on the potential or actual harm to adults or children at risk and the rationale for decision-making should always be recorded.</p> <p>When sharing information about adults, children and young people at risk between agencies it will only be shared :</p> <p>where relevant and necessary, not simply all the information held with the relevant people who need all or some of the information when there is a specific need for the information to be shared at that time</p>
How we collect (the source)and use the information	<p>The CCG may receive information relating to safeguarding concerns from you directly or relatives or through notification of concerns from other Health and Social Care organisations. All Health and Social Care professionals have a legal requirement to share information with appropriate agencies where safeguarding concerns about children or adults have been received. Where it is appropriate to do so the organisations will keep you informed of when information is required to be shared. Access to this information is strictly controlled and where there is a requirement to share information, e.g. with police or social services, all information will be transferred safely and securely ensuring only those with a requirement to know of any concerns are appropriately informed.</p>
Data Processors	<p>The CCG does not use external data processor s for this function.</p>
Your Rights	<p>With regards to Safeguarding under GDPR you have the right:</p> <p>To be informed about the processing of your information (this notice)</p> <p>Of access to the information held about you</p> <p>To have the information corrected in the event that it is inaccurate</p> <p>To be notified of data breaches</p>
How long we will keep the information	<p>Information is kept in accordance with the Records Management Code of Practice for Health and Social Care 2016 – depending on the nature of the records held, some records will be kept for longer than the standard retention periods within the Code of Practice.</p>
Who we will share the information with (recipients)	<p>Information will be shared with relevant professionals from partner agencies. Such as; Safeguarding Boards, Multi-Agency Safeguarding Hubs (MASH), Multi-Agency Risk Assessment Conference (MARAC), Local Authority, other Health and Social Care organisations or the Police</p>

Patient and Public Involvement

Data Controller(s)	NHS County Durham CCG
Purpose	If you have asked the CCG 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 through focus groups, meetings or surveys or are a patient representative in our groups, we will collect and use information you share with us. Where you submit your details to us for involvement purposes, we will only use your information for this purpose.
Type of information Used	Identifiable: Personal (such as name, address, date of birth)
Legal basis	GDPR Article 6 1(a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes
How we collect (the source) and use the information	We will be collecting and using your information to enable us to keep you informed of any news, consultation activities or patient participation groups. Your information will be held securely and accessible only to those who need it for the purposes it was collected.
Data Processors	Generally, the CCG does not use external data processors for this function. However, for bespoke or large scale exercises, the CCG may commission specialist data analyst companies to process information and produce reports. Any information shared with an external company would be transferred securely and only used for the agreed purpose.
Your Rights	With regards to Patient and Public Involvement under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information we hold about you. To have that information amended in the event that it is not accurate. To have the information deleted To restrict processing To object to processing/withdraw your consent for processing Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	We will only keep this information for as long as you are happy for us to do so, if you no longer wish us to use/ store your information you can request its removal/erasure at any time.
Who we will share the information with (recipients)	Your personal information will only be shared with CCG staff who need it for the purposes it was collected or, wider, with your permission and knowledge.

Serious Incident reports

Data Controller(s)	NHS County Durham CCG
Purpose	The CCG collects and uses information from Serious Incident reports from Primary and Secondary Care Providers to ensure incidents are dealt with appropriately and lessons learnt.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	<p>GDPR Article 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...' AND 6 (1) (c) – processing is necessary for compliance with a legal obligation...</p> <p>Related legislation:</p> <p>NHS Act 2006/Health and Social Care Act 2012.</p> <p>GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p>
How we collect (the source) and use the information	We are statutorily required to fully investigate and review incidents and will receive information from Primary and Secondary Care Providers. Where there is a requirement to provide incident reports externally, the information will be anonymised unless there is a legal requirement to provide your details. You will be kept informed of the requirements we are required to meet where information is to be shared externally.
Data Processors	The CCG Does not use external data processors for this function.
Your Rights	<p>With regards to Serious Incident Reports under GDPR you have the right:</p> <p>To be informed about the processing of your information (this notice)</p> <p>Of access to the information held about you</p> <p>To have the information corrected in the event that it is inaccurate</p> <p>Not to be subject automated decision-taking or profiling</p> <p>To be notified of data breaches</p>
How long we will keep the information	<p>Incidents (Serious) – 20 years</p> <p>Incidents (Other) – 10 years</p>
Who we will share the information with (recipients)	Your information may be shared with Primary and Secondary healthcare providers involved in the incident.

Freedom of Information requests

Data Controller(s)	NHS County Durham CCG
Purpose	As a public authority, the CCG has a duty to respond to requests made under the Freedom of Information Act 2000.
Type of information Used	Identifiable: Personal (such as name and address).
Legal basis	<p>GDPR Article 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...' AND 6 (1) (c) – processing is necessary for compliance with a legal obligation</p> <p>Relevant Legislation:</p> <p>The Freedom of Information Act 2000</p>
How we collect (the source) and use the information	<p>We will only collect identifiable information such as name and contact details provided by individuals making requests under the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR) and the Re-Use of Public Sector Information Regulations 2015 (RPSI). This information will only be used to respond to such requests and in correspondence with individuals following appeals.</p> <p>The personal data we process is freely provided by applicants who wish to exercise their right to use the above legislation in order to access information held by or on behalf of the CCG.</p> <p>Where the individual is making a request under the Re-Use of Public Sector Regulations 2015, by law we require the re-use purpose.</p>
Data Processors	The CCG uses NECS North of England Commissioning Support (NECS) as a Data Processor.
Your Rights	<p>With regards to Freedom of Information Requests under GDPR you have the right:</p> <p>To be informed about the processing of your information (this notice)</p> <p>Of access to the information held about you</p> <p>To have the information corrected in the event that it is inaccurate</p> <p>Not to be subject automated decision-taking or profiling</p> <p>To be notified of data breaches</p>
How long we will keep the information	<p>Freedom of Information (FOI) requests and responses and any associated correspondence - 3 years from the date of closure of the FOI request.</p> <p>FOI requests where there has been a subsequent appeal - 6 years from the date of closure of the appeal.</p>
Who we will share the information with (recipients)	This information is not shared outside of the CCG.

Medicines Management

Data Controller(s)	NHS County Durham CCG
Purpose	NHS County Durham CCG have a duty to secure continuous improvement in the quality of services provided to individuals for or in connection with the prevention, diagnosis or treatment of illness. Taking that into account, The medicines management team supports the CCG with commissioning services that make best use of available medicines. Your personal data will be used to fulfil this duty in respect of promoting cost-effective use of medicines as well as implementing projects or actions to optimise the use of medicines to improve outcomes, enhance patient safety and improve capacity within the local health economy.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	GDPR Article 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, GDPR Article 9 (2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.
How we collect (the source) and use the information	Data used to fulfil the above duties is received directly from the primary and secondary healthcare providers for which the CCG has responsibility for.
Data Processors	The CCG does not use external data processors for this function.
Your Rights	With regards to Medicines Management Reviews under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The organisation has adopted the retention periods for health and non-health care records as set out in the Records Management Code of Practice for Health and Social Care 2016. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016.
Who we will share the information with (recipients)	Personal data is shared between the CCG and local healthcare providers, including GP practices. They do this to facilitate the implementation of recommendations by the medicines management team.

Care and Treatment Reviews

Data Controller(s)	NHS County Durham CCG
Purpose	Care and Treatment Reviews (CTRs) are part of NHS England's commitment to transforming services for people with learning disabilities, autism or both. CTRs are for people whose behaviour is seen as challenging and/or for people with a mental health condition. They are used by commissioners for people living in the community and in learning disability and mental health hospitals.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller. GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.
How we collect (the source) and use the information	Care and Treatment Reviews involve pharmacists or pharmacy technicians reviewing patients' medication to gauge the appropriateness of the treatment they are receiving in order to reduce medicines-related harm or avoid unnecessary expenditure.
Data Processors	NHS County Durham CCG Other healthcare organisations involved with CTRs such as Local Authorities, Hospitals, Community Teams and GPs
Your Rights	With regards to Care and Treatment reviews under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The CCG will retain this information for a period of 8 years. The retention schedule is in line with the Records Management Code of Practice for Health and Social Care 2016.
Who we will share the information with (recipients)	Information may be shared with the Local Authority, and primary and secondary healthcare providers.

Referral Support Services

Data Controller(s)	NHS County Durham CCG
Purpose	When it has been identified by your GP or Optician that you require further diagnosis and/or treatment/care your GP/ Optician will make a referral to a secondary care service. For some specialties your referral will be reviewed by an independent specialist doctor to ensure that you receive the most effective care.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)
Legal basis	<p>GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller.</p> <p>GDPR Article 9(2)(h)- processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.</p>
How we collect (the source) and use the information	<p>The Referral Support Service involves a review of a copy of your GP referral against agreed clinical guidelines with the aim of ensuring the patient is seen by the right clinician, in the right place at the right time. These arrangements provide for an additional 'check' of referrals by a team of contracted clinicians. When you and your GP agree that you need a secondary care appointment, you can choose which hospital or clinic you go to. The Referral Support Service provides access to a system, (Choose and Book) that lets you choose your hospital or clinic and book your first appointment.</p> <p>This process is carried out with your consent in order to satisfy the Common Law Duty of Confidentiality.</p>
Data Processors	<p>e-RS Choose & Book Service</p> <p>Integrated Care Gateway – Accenda</p>
Your Rights	<p>With regards to the Referral Support Service under GDPR you have the right:</p> <ul style="list-style-type: none"> To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The CCG does not store this information. Referral letters are filed in the patient's record and held in accordance with the rules outlined in the Records Management: NHS Codes of Practice.
Who we will share the information with (recipients)	This information will be shared with NHS Service Providers and Independent Sectors if providing NHS Secondary Care Services.

Film and Promotional Materials

Data Controller(s)	NHS County Durham CCG
Purpose	We use this information to educate patients and the public on the services we provide.
Type of information Used	Identifiable – Name, face
Legal basis	GDPR Article 6 (1)(a) the data subject has given consent to the processing of his or her information for one or more specified purpose(s); GDPR Article 9(2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes,
How we collect (the source) and use the information	We will only collect and use this information with your consent. If you no longer wish for your information to be used for this purpose you can withdraw your consent at any time by contacting us at NECS North of England Commissioning Support (NECS)
Data Processors	The CCG does not use external Data Processors for this function.
Your Rights	With regards to Film & Promotional Materials under GDPR you have the right: To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To withdraw your consent to the processing. The right to data portability Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	The CCG will keep this information for a period of 5 years as documented on our consent form.
Who we will share the information with (recipients)	The majority of our film & promotional materials are available online via the CCGs website and are accessible/ viewable by the general public.

Information for Job Applicants

Data Controller(s)	NHS County Durham CCG
Purpose	The CCG will process information provided by applicants for the management of their application and the subsequent selection process.
Type of information Used	Anonymous – for shortlisting and selection purposes Identifiable: Personal such as name, address, date of birth etc.) - following the short-listing process
Legal basis	Article 6 – 6(1)(c) ‘...necessary for compliance with a legal obligation...’ For criminal conviction information (obtained via the Disclosure and Barring Service (DBS)) processing meets the requirements of Article 10 of the GDPR under Schedule 1, Part 1 of the Data Protection Act 2018 - processing in connection with employment, health and research - Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection. Relevant legislation: the provisions of the Safeguarding Vulnerable Groups Act 2006 as a basis for carrying our DBS checks.
How we collect (the source) and use the information	The recruitment process involves passing details provided by you on your application regarding your qualifications, skills and work experience, (but excluding your name, address and other personal data) to the short-listing and selection panels. After shortlisting full details provided by you on your application form will be provided to the interview panel. Details provided by you are also used to help fulfil our obligations to monitor equality and diversity within the organisation and process your application.
Data Processors	The CCG uses NECS North of England Commissioning Support (NECS) as a Data Processor.
Your Rights	To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To be notified of data breaches
How long we will keep the information	Recruitment records should be kept for a period of six months after the date of appointment.
Who we will share the information with (recipients)	We will share the information with recruiting managers.

Human Resources

Data Controller(s)	NHS County Durham CCG NHS Business Services Authority (for the Electronic Staff Record aspect)
Purpose	The CCG holds personal and confidential information on its staff for employment-related purposes, such as recruitment, payment of salary, sickness and absence monitoring and professional development purposes.
Type of information Used	Identifiable: Personal (such as name, address, date of birth) and Special Category (health, racial or ethnic origin information) Information relating to criminal convictions (DBS checks).
Legal basis	GDPR Article 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 AND 6 (1) (c) – Processing is necessary for compliance with a legal obligation... GDPR Article 9(2)(b) – processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment...social protection law in so far as it is authorised by Union or Member State law. For criminal conviction information (obtained via the Disclosure and Barring Service (DBS)) processing meets the requirements of Article 10 of the GDPR under Schedule 1, Part 1 of the Data Protection Act 2018 - processing in connection with employment, health and research - Processing necessary for the purposes of performing or exercising obligations or rights of the controller or the data subject under employment law, social security law or the law relating to social protection. Relevant legislation: the provisions of the Safeguarding Vulnerable Groups Act 2006 as a basis for carrying out DBS checks.
How we collect (the source) and use the information	The CCG uses information for the purposes of employment in a variety of ways including: Recruitment – application forms, collecting references, carrying out DBS checks, payroll and pension information. Managing and monitoring annual leave and sickness. Carrying out personal development reviews. Referrals to Occupational Health Disciplinary procedures. Processing staff leavers, retirements and providing references. Recruitment of temporary staff/student placements
Data Processors	Northumbria FT

OFFICIAL

	<p>The CCG uses NECS North of England Commissioning Support (NECS) as a Data Processor.</p> <p>IBM (system supplier of the Electronic Staff Record - ESR)</p> <p>NHS Business Services Authority – management of NHS Jobs (recruitment website)</p> <p>Northumbria FT (finance system) for payroll purposes</p>
Transfer of information overseas	<p>NHS SBS carry out some of their processing activity in India. Where this occurs it is governed by the use of approved Model Contract Clauses.</p>
Your Rights	<p>Under GDPR you have the right:</p> <p>To be informed about the processing of your information (this notice)</p> <p>Of access to the information held about you</p> <p>To have the information corrected in the event that it is inaccurate</p> <p>To be notified of data breaches</p>
How long we will keep the information	<p>The CCG will store this information for a period of 5 years after the termination of employment.</p>
Who we will share the information with (recipients)	<p>In addition to the sharing with our named Data Processors above - the CCG shares information with a variety of organisation and individuals for a number of lawful purposes including:</p> <p>Public disclosure under Freedom of Information - e.g. requested names or contact details of senior managers or those in public-facing roles;</p> <p>Disclosure of job applicant details - e.g. to named referees for reference checks, to the Disclosure & Barring Service for criminal record checks</p> <p>Disclosure to employment agencies - e.g. in respect of agency staff;</p> <p>Disclosure to banks & insurance companies - e.g. to confirm employment details in respect of loan/mortgage applications/guarantees;</p> <p>Disclosure to professional registration organisations - e.g. in respect of fitness to practice hearings;</p> <p>Disclosure to Occupational Health professionals (subject to explicit consent);</p> <p>Disclosure to police or fraud investigators - e.g. in respect of investigations into incidents, allegations or enquiries.</p>

Declarations of Interests, Gifts and Hospitality Publication

Data Controller(s)	NHS County Durham CCG
Purpose	The CCG is required to maintain and publish on its website registers of interests, gifts and hospitality for all staff of the CCG, as well as its Members, Governing Body and Committee Members
Type of information Used	Identifiable: Personal (name and job role)
Legal basis	GDPR Article 6(1)(c) processing is necessary for compliance with a legal obligation; Statutory guidance for CCGs on Managing Conflicts of Interest under Section 140 of the National Health Service Act 2006 (as amended by the Health and Social Care Act 2012)
How we collect (the source) and use the information	The CCG maintains and publishes Registers of Interest and Gifts and Hospitality containing names, job roles, details of the interest and/or receipt of gifts/hospitality including the details of those supplying the gift/hospitality as per the guidance on Managing Conflicts of Interest.
Data Processors	The CCG does not use external data processors for this function.
Your Rights	<p>In exceptional circumstances, where the public disclosure of information could lead to a real risk of harm or is prohibited by law, a person's name or other information may be withheld from the published registers. If you feel that substantial damage or distress may be caused to you or somebody else by the publication of information in the registers, you are entitled to request that the information is not published. Such requests must be made in writing to the CCG.</p> <p>Under GDPR you have the right:</p> <ul style="list-style-type: none"> To be informed about the processing of your information (this notice) Of access to the information held about you To have the information corrected in the event that it is inaccurate To restrict or stop processing To object to it being processed or used Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	CCG must retain a private record of historic interests and offers/receipt of gifts and hospitality for a minimum of 6 years after the date on which it expired.
Who we will share the information with (recipients)	<p>The registers are published on the CCG's website.</p> <p>Information may be shared with NHS England.</p>

National Fraud Initiative

Data Controller(s)	NHS County Durham CCG
Purpose	<p>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 under the National Fraud Initiative.</p> <p>The Cabinet Office is responsible for carrying out data matching exercises.</p>
Type of information Used	Identifiable: Personal
Legal basis	<p>GDPR Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.</p> <p>Relevant Legislation: Part 6 of the Local Audit and Accountability Act 2014 (LAAA).</p>
How we collect (the source) and use the information	<p>We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise, as detailed here.</p> <p>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.</p> <p>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>Data matching by the Cabinet Office is subject to a Code of Practice.</p> <p>For further information on data matching at this authority, contact the CCG's Corporate Services Manager</p>
Data Processors	<p>The Cabinet Office</p> <p>The Cabinet Office</p> <p>National Fraud Initiative – You can find more information about how the NFI use your data here.</p>
Your Rights	<p>Under GDPR you have the right:</p> <p>To be informed about the processing of your information (this notice)</p> <p>Of access to the information held about you</p>

OFFICIAL

	To have the information corrected in the event that it is inaccurate To be notified of data breaches
How long we will keep the information	The datasets used in the matching exercise by the Cabinet Office will be kept as per the Code of Data Matching Practice
Who we will share the information with (recipients)	The Cabinet Office and Counter Fraud Authority

APPENDIX B

Glossary

Aggregated – grouped information about individuals that has been combined to show general trends or values without identifying individuals.

Anonymised - data which is about you but from which you cannot be personally identified.

Caldicott Guardian – a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. Each NHS and Social Care organisation is required to have a Caldicott Guardian.

Data Controller – natural or legal person, public body, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor – natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

Data Protection Act – UK legislation to be introduced in 2018 in line with GDPR to expand on the EU Regulation and to provide for areas specifically excluded from GDPR (e.g. Law Enforcement). This Act will repeal the UK Data Protection Act 1998.

Data Protection Officer – Under GDPR all Public Authorities must appoint a Data Protection Officer. The role of this person, who must be an expert in Data Protection Law, is :

- Monitor CCG compliance with the GDPR
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the GDPR such as the principles of data processing, data subjects' rights, privacy impact assessments, records of processing activities, security of processing and notification and communication of data breaches

General Data Protection Regulation (GDPR) – the main legislation on data protection binding all EU member states (including the UK) from May 2018.

Identifiable - information which contains personal details that identify individuals such as name, address, email address, NHS Number, full postcode, date of birth.

Personal data – 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 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.

Primary Care - Primary care settings include GP Practices, pharmacists, dentists and some specialised services such as military health services.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as collection, recording, organisation,

OFFICIAL

structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pseudonymised - individual level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity.

Right of Access Requests – The right a data subject has from the controller for confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and further information about the processing.

Secondary Care - Secondary care settings include local hospitals, rehabilitative care, urgent and emergency care (including out of hours and NHS 111), community and mental health services.

Senior Information Risk Owner (SIRO) – an executive or member of the Senior Management Board of an organisation with overall responsibility for information risk across the organisation.

Special Category (Sensitive) data - categories of personal data for which special safeguards are required by law. This includes records relating to health, sex life, race, ethnicity, political opinions, trade union membership, religion, genetics and biometrics.