

Privacy Notice

How your personal information is used by NHS Sheffield CCG

Please click on the highlighted text within the notice for links to further information. Click the link for a [Glossary](#) of definitions used throughout this notice.

Who we are and what we do

Data Controller: NHS Sheffield Clinical Commissioning Group
Address: 722 Prince of Wales Road
Sheffield
S9 4EU

Data Protection Officer (DPO): EMBED DPO Shared Service
DPO Contact Details: embed.gdpr@nhs.net

NHS Sheffield Clinical Commissioning Group is responsible for planning and designing local health services in and around Sheffield. We do this by 'commissioning' or buying health and care services including:

- Planned hospital care
- Unplanned care (urgent care)
- Rehabilitation care
- Community Health Services
- Mental Health and learning disability services

We are also responsible for arranging unplanned care services for our registered patients and for commissioning services for any unregistered patients who live in Sheffield. All General Practices in Sheffield belong to our Clinical Commissioning Group.

We manage the performance of services that we commission to make sure that they are safe, provide high quality care and meet the needs of local people. Part of this performance management role includes responding to any concerns from our patients about these services.

How we use your personal information

The purpose of this notice is to inform you of the type of information (including personal information) that the CCG holds as a Data Controller, how that information is used, the legal basis for using the information, who we may share that information with, and how we keep it secure and confidential.

It covers information we collect directly from you or collect indirectly from other individuals or organisations for the CCG's registered population.

This notice applies to all information held by the CCG relating to individuals, whether you are a patient, service user or a member of staff. This notice was last reviewed in Sep 2018.

Types of information we hold

We need to use information about you in various forms and will only use the minimum amount of information necessary for that purpose. Where possible we will use information that does not identify you.

The CCG uses and processes several different types of information, (details below for more information):

1. Anonymised - data which is about you but from which you cannot be personally identified.
2. Pseudonymised - individual level information where individuals can be distinguished by using a coded reference, which does not reveal their 'real world' identity
3. Identifiable - information which contains personal details that identify individuals such as name, address, email address, NHS Number, full postcode, date of birth.
4. Aggregated – grouped information about individuals that has been combined to show general trends or values without identifying individuals

Throughout this Notice you will see reference to an organisation called NHS Digital. They are the national body responsible for information, data and information processing in health and social care. NHS Digital has legal responsibility for identifiable data to be passed securely to them by Primary and Secondary Care Providers who are legally obliged to provide this information.

Details of information used for specific purposes

Use of Anonymised Data

We use anonymised data to plan health care services including:

- Checking the quality and efficiency of the health services we commission;
- Preparing performance reports on the services we commission;
- Working out what illnesses people will have in the future, so we can plan and prioritise services and ensure these meet the needs of patients;
- Reviewing the care being provided to make sure it is of the highest standard.

Use of Pseudonymised (De-identified) Information

We use de-identified information in our role as commissioner including:

- **Commissioning** - to plan, design, contract for and pay for the best possible care available for you ; look at the care provided by different providers across our area to make sure that together they support the needs of the local population; performance manage contracts; to prepare statistics on NHS performance to understand health needs and support service redesign, modernisation and improvement; to help us plan future services to ensure they continue to meet our local population needs
- **Risk Stratification**- to identify groups of patients who would benefit from some additional help from their GP or care team. The aim is to prevent ill health and possible future hospital stays, rather than wait for you to become sick. Only de-identified information is accessible to the CCG in order to help us plan the most appropriate health services for our population.

Use of Personal and Sensitive (Identifiable) Information

As a CCG we do not routinely hold medical records or confidential patient data with some limited exceptions.

There are some categories of personal data for which special safeguards are required by law, known as special category or sensitive data. This includes records relating to health, sex life, race, ethnicity, political opinions, trade union membership, religion, genetics and biometrics.

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.

Patient Information

- [Invoice Validation](#)
- [Complaints](#)
- [Individual Funding requests \(IFR\)](#)
- [Continuing Healthcare](#)
- [Personal Health Budgets \(PHBs\)](#)
- [Safeguarding](#)
- [Patient and Public Involvement](#)
- [Infection Prevention and Control](#)
- [Serious Incident reports](#)
- [Freedom of Information requests](#)
- [Assuring Transformation \(Learning Disability Data\)](#)
- [Medicines Management](#)
- [Care and Treatment Reviews](#)
- [Visitors to our Website](#)

Staff Information

The CCG as an NHS Employer needs to process information in relation to staff. This information is used in a variety of ways to ensure staff are paid, that the CCG complies with employment law, or to provide other services related to their employment. For more details about how staff information is used please click on the following:

- [Information for Job Applicants](#)
- [Human Resources](#)
- [Declarations of Interests, Gifts and Hospitality Publication](#)
- [National Fraud Initiative](#)

Children Information

Please see the links on our website for our Privacy Notice for Teens or younger children

Sharing Information with Health and Care organisations

Information Sharing Agreements and contracts will be in place ensuring that where we share information, this meets both the requirements of the Health and Social Care Act 2012 and the current Data Protection legislation ensuring that your confidentiality and rights are not breached.

The CCG is actively working with health and social care partners to ensure that where you receive a referral, for example for community services, all the relevant information that organisation requires in order to offer you the right service is available. We are also working with the hospitals that provide services to our population to ensure that if you find yourself in an emergency situation, relevant and potentially lifesaving information from your GP record will be available, showing any latest tests and any allergies you may suffer from, which the hospital clinicians will need to know.

Whenever a new arrangement is made to share information externally, both with health and social care organisations and with third party suppliers, we will ensure that a legal basis has been identified, using a tool called a Data Protection Impact Assessment, which will highlight any risks to your information and ensure they are resolved before any sharing takes place.

Our Commitment to Data Privacy and Confidentiality

We are committed to protecting your privacy and will only process personal confidential data in accordance with the General Data Protection Regulation, the Data Protection Act 2018, the Common Law Duty of Confidentiality, Professional Codes of Practice and the Human Rights Act 1998.

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

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

Everyone working for the NHS has a legal and contractual duty to keep information about you confidential.

All identifiable information that we hold about you will be held securely and confidentially. We use administrative and technical controls to do this. All health and social care organisations are required to provide annual evidence of compliance with applicable laws, regulations and standards through the Data Security and Protection toolkit.

Our staff, contractors and committee members receive appropriate and ongoing training to ensure that they are aware of their personal responsibilities and have contractual obligations to uphold confidentiality, enforceable through disciplinary procedures. Staff are trained to ensure how to recognise and report an incident and the organisation has procedures for investigating, managing and learning lessons from any incidents that occur.

Your information will not be sent outside of the United Kingdom, unless your privacy is protected to the same extent as the law in the UK. We will never sell any information about you.

The CCG maintains a set of regularly updated policies and procedures covering all aspects of information governance. These can be found here:

<http://www.sheffieldccg.nhs.uk/about-us/publications-scheme.htm>

Your Rights

Under the General Data Protection Regulation all individuals have certain rights in relation to the information which the CCG holds about them. Not all rights apply equally to all our processing activity as certain rights are not available depending on the lawful basis for the processing.

When you view an entry in our 'Use of Personal and Sensitive Information', we have highlighted which rights apply and which may not. To help understand why some may not apply the following should help.

Examples of where rights may not apply - where our lawful basis is:

- Processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller - then rights of erasure, portability do not apply.
- Legal Obligation - then rights of erasure, portability, objection, automated decision making and profiling do not apply.

If you require further detail each link below will take you to the Information Commissioner's Office's website where further detail is provided in section 'When does the right apply'.

These rights are:

- [The right to be informed about the processing of your data](#)
- [The right of access to the data held about you](#)
- [The right to have that information amended in the event that it is not accurate](#)
- [The right to have the information deleted](#)
- [The right to restrict processing](#)
- [The right to have your data transferred to another organisation \(data portability\)](#)
- [The right to object to processing](#)
- [Rights in relation to automated decision making and profiling](#)

Under the [NHS Constitution](#) you have the right to privacy and to expect the NHS to keep your information confidential and secure.

You have the right to be informed about how your information is used.

You have the right to request that your confidential information is not used beyond your own care and treatment, and to have your objections considered and where your wishes cannot be followed, to be told the reasons including the legal basis.

There is a new national opt-out that allows people to opt out of their confidential patient information being used for reasons other than their individual care and treatment. The system offers patients and the public the opportunity to make an informed choice about whether they wish their personally identifiable data to be used just for their individual care and treatment or also used for research and planning purposes. Details of the national patient opt out can be found here: <https://www.nhs.uk/your-nhs-data-matters/>

Queries and Complaints

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

If you have any questions or complaints regarding the information we hold about you or the use of your information, please contact:

Complaints Team
NHS Sheffield CCG
722 Prince of Wales Road
Sheffield
S9 4EU

Or via email: SHECCG.complaints@nhs.net

DATA PROTECTION OFFICER – QUERIES REGARDING DATA PROTECTION ISSUES

New legislation (General Data Protection Regulation and Data Protection Act 2018) mandates that the CCG appoint a Data Protection Officer (DPO). This is because we are a public body.

The DPO will assist us to monitor internal compliance, inform and advise on data protection obligations and act as a contact point for data subjects (members of the public and employees) where there are concerns or queries regarding Data Protection. The DPO will also act as a contact point for communication with the Information Commissioner's Office.

The CCG has appointed a shared service to deliver the DPO role provided by eMBED Health Consortium

June 2019

If you wish to contact the DPO then please use the following contact details stating in the heading which organisation you are enquiring about:

embed.gdpr@nhs.net

For independent advice about data protection, privacy and data-sharing issues, or to make a complaint about our handling of your information you can contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Phone: 0303 1231113 or 01625 54 57 45

Website: <https://ico.org.uk/>

Details of information used for specific purposes

Commissioning

Data Controller(s)	NHS Sheffield 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	Different types of commissioning data are legally allowed to be used by different organisations within, or contracted to, the NHS. Identifiable – when disclosed from Primary and Secondary care services to NHS Digital Pseudonymised – the CCG may only receive this information in a pseudonymised format which does not identify individuals.
Legal Basis	Statutory requirement for NHS Digital to collect identifiable information. For use by the CCG: 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 from the Secretary of State, through the Confidentiality Advisory Group , enables the pseudonymised information to be sent to the CCG via NHS Digital for our Commissioning purposes.
How we collect (the source) and use the information	The datasets we receive from NHS Digital have been linked and are in a format that does not directly identify you. Information such as your age, ethnicity and gender, as well as coded information about any clinic or Accident and Emergency attendances, hospital admissions and treatment will be included. We also receive information from the GP Practices within our CCG that does not identify you. We use these datasets for a number of purposes such as: Performance managing contracts Reviewing the care delivered by providers to ensure service users are receiving quality and cost effective care To prepare statistics on NHS performance to understand health needs and support service redesign, modernisation and improvement To help us plan future services to ensure they continue to meet our local population needs
Data Processors	Yorkshire Data Services for Commissioning Regional Office (DSCRO) hosted by North of England Commissioning Support (NECS) 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 the CCG.

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. There are different types or levels of opt-out available; Type 1 opt out is where you do not wish for your information to be shared outside of your GP Practice for any purpose other than your direct care and Type 2 opt out is where you do not wish for your information to be shared by NHS Digital.</p> <p>From 25 May 2018 the type 2 opt-out has been replaced by the National Data Opt-Out with a transition period running until October 2018. Type 2 opt-outs that have been recorded previously have been automatically converted to national data opt-outs. Further information about the Type 2 opt-out and the conversion to the national data opt-out is available from NHS Digital. 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>Information is retained in accordance with the Records Management Code of Practice for Health and Social Care 2016. Datasets received via NHS Digital are retained for as long as the Data Sharing Agreement is in place.</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)	<p>NHS Sheffield CCG</p>
Purpose	<p>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.</p>
Type of information Used	<p>Only de-identified information (NHS number removed) is accessible to the CCG.</p> <p>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.</p>
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</p>

	<p>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 (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.</p>
How we collect (the source) and use the information	<p>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. This information is passed to eMBED Health Consortium who provides the Risk Stratification tool to GP Practices on behalf of the CCG.</p> <p>De-identified information is made available to the CCG to provide a picture of the health and needs of their local population, which enables:</p> <p>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.</p>
Data Processors	<p>Data Services for Commissioners Regional Office (DSCRO) hosted by North of England Commissioning Support (NECS) North of England Commissioning Support (NECS) eMBED Health Consortium</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. There are different types or levels of opt-out available; Type 1 opt out is where you do not wish for your information to be shared outside of your GP Practice for any purpose other than your direct care and Type 2 opt out is where you do not wish for your information to be shared by NHS Digital. From 25 May 2018 the type 2 opt-out has been replaced by the national data opt-out. Type 2 opt-outs that have been recorded previously have been automatically converted to national data opt-outs. Further information about the Type 2 opt out and the conversion to the national data opt-out is available from NHS Digital.</p> <p>Details of the national patient opt 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 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>Information is retained in accordance with the Records Management Code of Practice for Health and Social Care 2016. Datasets received</p>

	via NHS Digital are retained for as long as the Data Sharing Agreement is in place
Who we will share the information with (recipients)	This information is not shared outside of the CCG

Invoice Validation

Data Controller(s)	NHS Sheffield 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 of their service 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), hosted on our behalf by NHS Rotherham CCG, 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 (CAG 7-07(a)(b)(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 (Controlled Environment for Finance) 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 Controlled Environment for Finance 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	<p>NHS Rotherham CCG who operate the Controlled Environment for Finance as a shared service.</p> <p>NHS Shared Business Services - used by the Controlled Environment for Finance as a Data Processor</p>
Transfers of Data Overseas	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.
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.</p> <p>Type 2 opt outs apply to invoice validation - where you do not wish for your information to be shared by NHS Digital.</p> <p>From 25 May 2018 the type 2 opt-out has been replaced by the national data opt-out. Type 2 opt-outs that have been recorded previously have been automatically converted to national data opt-outs. Further information about the Type 2 opt out and the conversion to the national data opt-out is available from NHS Digital. Details of the national patient opt out can be found here: https://www.nhs.uk/your-nhs-data-matters/</p> <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 you • To have the information corrected in the event that it is inaccurate • 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	Invoices are retained for 6 years after the end of the financial year to which they relate.
Who we will share the information with (recipients)	This information is not shared outside of the CCG.

Complaints

Data Controller(s)	NHS Sheffield 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 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	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

	<p>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. 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	None
Your Rights	<p>With regards to Complaints 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 • 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	Complaint files are kept for a maximum of ten 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 Sheffield 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, NHS number) 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	Blueteq Ltd
Your Rights	With regards to Individual Funding Requests under GDPR you have the right: <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	Information relating to Individual Funding requests where the funding has been granted will be retained as per the standard care records retention set out in the Records Management Code of Practice for Health and Social Care 2016 . Where requests have been rejected information will be retained for 2 years.
Who we will share the information with (recipients)	This information is not shared outside of the CCG.

Continuing Healthcare (CHC)

Data Controller(s)	NHS Sheffield CCG
Purpose	Where you have asked us to undertake assessments for Continuing

	Healthcare – a package of care for those with complex medical needs. We use your information in order to be able to make the appropriate arrangements for resulting care packages.
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. The consent of the patient or their legal representative, is obtained to satisfy the Common Law Duty of Confidentiality.
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.
Data Processors	QAPLus Ltd - Suppliers of the QA CHC records system TPP - suppliers of SystmOne electronic patient records system NHS Doncaster CCG for the administration of Previously Unassessed Periods of Care (Retrospective CHC) funding requests as well as all related appeals
Your Rights	With regards to Continuing Healthcare under GDPR you have the right: <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	Information relating to Continuing Healthcare/ Section 117 requests where the funding has been granted will be retained as per the standard care records retention set out in the Records Management Code of Practice for Health and Social Care 2016 . Where requests have been rejected information will be retained for 2 years.
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 Sheffield CCG
Purpose	A Personal Health Budget is an amount of money allocated to pay for your health and wellbeing needs agreed between you and your local NHS team. Personal Health Budgets help people with long term health conditions manage their care and support in a way that suits them. It helps them to have more choice and flexibility in the way

	<p>their care and support needs are met. Any adult or child who is eligible for NHS Continuing Healthcare can have a Personal Health Budget if they want one. There are plans to widen the availability of Personal Health Budgets in the future.</p>
Type of information Used	<p>Identifiable: Personal (such as name, address, date of birth) and Special Category (health information)</p>
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>Personal Health Budgets are managed in one of three ways or a combination of all three.</p> <ul style="list-style-type: none"> • Notional - We tell you how much money is available for your care; you say how you want us to spend the money. If your local NHS team agree this meets your needs they arrange the care and support for you. • Third Party - An organisation looks after the money for you and you say how you want to spend it. If your local NHS team agrees this meets your needs, the organisation pays for the care and support you have chosen. • Direct Payments - Once your care plan has been agreed, we give you or your representative the money to buy and manage your own healthcare and support. Your local NHS team must agree that this meets your needs. <p>You can spend your Personal Health Budget on any care or services that are set out in your care plan and agreed with your local NHS team. You will be able to use your Personal Health Budget for a range of things to help you meet your goals, for example therapies, personal care and equipment. You don't have to change the healthcare and support that is working well for you, but if there is something that isn't working, you can change that.</p> <p>Things you can't include in your plan will be explained to you at the beginning of the planning process. You will not need to pay for emergency care and care you normally get from a GP.</p> <p>This process is carried out with the consent of the patient to satisfy the Common Law Duty of Confidentiality.</p>
Data Processors	<p>Sheffield City Council who arrange and administer jointly funded packages of care agreed as part of the PHB scheme.</p>
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	<p>Information relating to Personal Health Budgets where the funding</p>

information	has been granted will be retained as per the standard care records retention set out in the Records Management Code of Practice for Health and Social Care 2016 . Where requests have been rejected information will be retained for 2 years.
Who we will share the information with (recipients)	Sheffield City Council and other health and care organisations involved in delivering or arranging the care required. The third party looking after your money where this has been arranged.

Safeguarding

Data Controller(s)	NHS Sheffield CCG
Purpose	Information for safeguarding purposes is used to assess and evaluate safeguarding concerns to ensure individuals (children and adults at risk of abuse or neglect) within the CCG's boundaries are effectively protected.
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)(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..' For the purposes of Article 9(2)(b) the provisions of the Children Acts 1989 and 2004, and the Care Act 2014 are relevant.
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, to be provide you with assurance regarding the security of that sharing and the benefit to you or the person you are raising safeguarding concerns about. 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> <p>The Children Act 1989 establishes implied powers for local authorities to share information to safeguard children. Local authorities have a duty to investigate where a child is the subject of an emergency protection order, is in police protection or where there is reasonable cause to suspect that a child is suffering or is likely to suffer significant harm.</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</p>

	<p>Act 2004 local authorities must make arrangements to promote cooperation with relevant partners and others, to improve well-being.</p> <p>The Care Act 2014 outlines the responsibilities of organisations to comply with requests for information from the Safeguarding Adults Board to enable or assist the Board to exercise its functions. This may include information required to undertake a Safeguarding Adult Review.</p> <p>The statutory guidance to the Care Act emphasises that early sharing of information is the key to providing an effective response where there are emerging concerns, and that partner organisation 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>
Data Processors	None
Your Rights	<p>With regards to Safeguarding 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 be notified of data breaches
How long we will keep the information	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.
Who we will share the information with (recipients)	Information may be shared with Safeguarding Boards, Multi-Agency Safeguarding Hubs (MASH), Multi-Agency Risk Assessment Conference (MARAC), Local Authority, other Health and Social Care organisations or the Police.

Patient and Public Involvement

Data Controller(s)	NHS Sheffield 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 or patient participation 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) Special Category (health information) voluntarily disclosed as part of personal views and care experiences
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>Relevant legislation – Health and Social Care Act 2012 – CCGs have a statutory duty to consult with the public.</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 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. Information provided about care experience will not be disclosed in an identifiable manner without your explicit written consent
Data Processors	Survey Monkey survey hosting and reporting Mailchimp Bulk email, engagement management, click analysis Twitter Click Analysis Eventbrite Event management Facebook Click Analysis SiteKit Ltd Website hosting Traktivity Contacts information FrankLTD Website design / hosting
Your Rights	With regards to Patient and Public Involvement under GDPR you have the right: <ul style="list-style-type: none"> • 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	Information in relation to public consultations will be kept for 5 years following the end of the consultation. Membership database data will kept for two years after last explicit consent obtained
Who we will share the information with (recipients)	No sharing outside of the CCG

Infection Prevention and Control

Data Controller(s)	NHS Sheffield CCG
Purpose	CCGs collaborate with Public Health services and work closely with the organisations involved in providing patient care, to jointly identify and agree the possible causes of, or factors that contributed to a patient's infection.
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)(j) '...necessary for reasons of public interest in the area of public health...or ensuring high standards of quality and safety of health care and of medicinal products or medical devices...'

	<p>Related legislation: The Health and Social Care Act 2008: Code of Practice for the NHS for the Prevention and Control of Healthcare Associated Infections (revised January 2015) and Regulation 3 of The Health Service (Control of Patient Information) Regulations 2002</p>
How we collect (the source) and use the information	<p>CCGs participate in Post Infection Review in the circumstances set out in the Post Infection Review Guidance, issued by NHS England. The CCG receives this information from Healthcare providers. The CCG uses the results of the Post Infection Review to inform the mandatory healthcare associated infections reporting system.</p>
Data Processors	
Your Rights	<p>With regards to Infection Prevention and Control 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 • Not to be subject automated decision-taking or profiling • To be notified of data breaches
How long we will keep the information	<p>Post infection reviews may be kept for up to six years.</p>
Who we will share the information with (recipients)	<p>Information may be shared with Primary and Secondary healthcare providers and with the Local Authority who are responsible for Public Health with the CCG boundary.</p>

Serious Incident reports

Data Controller(s)	NHS Sheffield 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...'</p> <p>Related legislation: NHS Act 2006/Health and Social Care Act 2012. 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>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.</p>

Data Processors	None
Your Rights	With regards to Serious Incident Reports under GDPR you have the right: <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 • Not to be subject automated decision-taking or profiling • To be notified of data breaches
How long we will keep the information	30 Years from Date of Incident
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 Sheffield CCG
Purpose	As a public authority, the CCG has a duty to respond to requests made under the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 (EIR), and the Re-Use of Public Sector Information Regulations 2015 (RPSI).
Type of information Used	Identifiable: Personal (name and either email or postal address only)
Legal basis	GDPR Article 6(1)(c) 'processing is necessary for compliance with a legal obligation to which the controller is subject' Relevant legislation: FOIA, EIR and RPSI.
How we collect (the source) and use the information	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. 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. Where the individual is making a request under the Re-Use of Public Sector Regulations 2015, by law we also require the name of the organisation and the re-use purpose.
Data Processors	None
Your Rights	With regards to Freedom of Information Requests under GDPR you have the right: <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	FOIA requests and associated responses will be kept for 3 years

information	following the closure of the request except in cases where there has been a subsequent appeal. For those cases, information will be kept for 6 years following the closure of the appeal.
Who we will share the information with (recipients)	This information is not shared outside of the CCG.

Assuring Transformation (Learning Disability Data)

Data Controller(s)	
Purpose	Assuring Transformation (AT) data collects information about individuals with learning disabilities and/or autism, who may have a mental health condition or behaviour that challenges, in in-patient settings, and provides it to the CCG. It gives the CCG broad oversight of their 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>It is a statutory duty for the CCG to participate in this data collection. There are formal directions from the Secretary of State mandating the collection: (Health & Social Care Act 2012) – in the General Guidance. The Information Standard Notice for this data collection was published on 6th January 2015 (SCCI2007 Amd 7/2014).</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 (CAG 8-02(a-c)/2014) from the Secretary of State, through the Confidentiality Advisory Group, enables the flow of personal confidential data from organisations to commissioners, about the services that they provide for:</p> <ul style="list-style-type: none"> • people in in-patient beds with learning disabilities and/or autism of, • any age • any level of security (general / low / medium / high) • any status under the Mental Health Act (informal or detained) <p>However, the information cannot be shared if:</p> <ul style="list-style-type: none"> • the individual has objected to the use of their information as part of the AT data • the individual lacks capacity to make their own decision
How we collect (the source) and use the information	The AT data is sent to the CCG from healthcare providers and collected by NHS Digital on NHS England's behalf. It covers all people with learning disabilities and/or autism that are being cared for in in-patient settings and includes: the number of people in in-patient settings; discharges and admissions; whether individuals have a care plan, a care co-ordinator, regular care reviews and access to independent advocacy; the age and gender of individuals; and the type of in-patient setting that is providing their care. The information collected is published in reports by NHS Digital. The reports don't include any personal information, like names, birthdays or NHS numbers in them.

Data Processors	
Your Rights	<p>Under the NHS constitution you have the right to be informed about how your information is used. You also have the right to request that your confidential information is not used beyond your own care and treatment, and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis. If you do not wish for your information to be included in the information sent to NHS Digital then please let us know via Owen Jones (owen.jones2@nhs.net)</p> <p>With regards to Assuring Transformation 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	
Who we will share the information with (recipients)	Information will be received from healthcare providers and shared with NHS Digital and NHS England.

Medicines Management

Data Controller(s)	NHS Sheffield CCG
Purpose	<p>Controlled Drugs Monitoring - The CCG has a duty to assist the relevant Controlled Drug Accountable Officer (CDAO) of NHS England in the carrying out of the CDAO's functions under The Controlled Drugs (Supervision of Management and Use) Regulations 2013. These regulations aim to strengthen the governance arrangements for the use and management of controlled drugs.</p> <p>Minor Ailments - The Minor Ailments Scheme enables you to receive prescription medications, to treat a range of common conditions, direct from the pharmacist without a GP prescription.</p>
Type of information Used	Pseudonymised information 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>Relevant legislation: The Controlled Drugs (Supervision of Management and Use) Regulations 2013</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>

	Common Law Duty of Confidentiality – for Controlled Drugs Monitoring it is a legal requirement for the CCG to undertake this work under The Controlled Drugs (Supervision of Management and Use) Regulations 2013
How we collect (the source) and use the information	Community Pharmacists enter records of patients seen along with their medical condition. The pseudonymised version are shared for payment and service planning purposes
Data Processors	UKFAST web hosting
Your Rights	With regards to Medicines Management under GDPR you have the right: <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 • Not to be subject automated decision-taking or profiling To be notified of data breaches
How long we will keep the information	Locally held controlled drugs information will be kept for 7 years. NHS England and NHS Business Services Authority guidance for controlled drugs can be found at: http://www.nhsbsa.nhs.uk/PrescriptionServices/1120.aspx and https://www.england.nhs.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf NHS BSA will keep primary data on controlled drugs for 20 years then review.
Who we will share the information with (recipients)	This information is shared between GP Practices, the CCG and NHS England.

Care and Treatment Reviews

Data Controller(s)	
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	
How we collect (the source) and use the information	Care and Treatment Reviews are independent panel meetings about your care arranged by the CCG. The CTR panel is made up of professionals who are not involved in your everyday care. The panel members listen to you and to everyone involved in your care. They look at your notes and check that your care and plans are working well. They use this information and their own experience to decide what will improve your care and plans for the future. They speak up when they think your care could be different or better. CCGs have to understand people's needs, to plan for different levels of support at different times. They work with other health and social care services to find out who needs extra support or contact to make sure things are okay. This list or register helps the CCG work with

	<p>health and social care services. It allows them to arrange the extra support needed, if a CTR is needed, or extra help for carers. If you need a community CTR, you can join this register. Ask your care co-ordinator about it.</p> <p>If someone suddenly becomes very unwell and urgently needs to go into hospital, there might not be enough time for a community CTR. If this happens, an adult should have a hospital CTR within four weeks of going into hospital, or two weeks if you are a child or young person. This process is carried out with consent from the patient in order to satisfy the Common Law Duty of Confidentiality.</p>
Data Processors	
Your Rights	<p>With regards to Care and Treatment reviews 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	
Who we will share the information with (recipients)	Information may be shared with the Local Authority, and primary and secondary healthcare providers.

Visitors to our Website

Data Controller(s)	NHS Sheffield CCG
Purpose	Monitoring how the CCG's website is used. This is done to find out things such as the number of visitors to the various parts of the site.
Type of information Used	Identifiable: Personal (IP address)
Legal basis	GDPR Article 6(1)(f) – processing is necessary for the purposes of the legitimate interests pursued by the Controller
How we collect (the source) and use the information	<p>When someone visits the CCG's website information is collected in a standard internet log to enable the CCG to monitor how the website is used. This is done to find out things such as the number of visitors to the various parts of the site.</p> <p>From time to time, you may be asked to submit personal information about yourself (e.g. name and email address) in order to receive or use services on our website. Such services include bulletins, email updates, website feedback, requesting investigation of complaints and any other enquiries.</p> <p>By entering your details in the fields requested or sending us an email, you enable the CCG and its service providers to provide you with the services you select. Any information you provide will only be used by the CCG, or our agents or service providers, and will not be disclosed to other parties unless we are obliged or permitted to do</p>

	<p>so.</p> <p>We will hold your personal information on our systems for as long as you use the service you have requested, and remove it in the event the purpose has been met or when you no longer wish to continue your subscription.</p>
Data Processors	<p>SiteKit Ltd Website hosting Google LLC Website Analytics Mailchimp Bulk email management and click analysis Twitter Click analysis Facebook Click analysis Traktivity Contacts information FrankLTD Website design / hosting</p>
Your Rights	<p>Under GDPR you have the right:</p> <ul style="list-style-type: none"> To be informed about the processing of information (this notice) <p>To object to it being processed. There are legitimate reasons why we may refuse your objection, which depend on why we are processing it.</p>
How long we will keep the information	Five years or until deletion requested
Who we will share the information with (recipients)	Not shared outside of the CCG

Information for Job Applicants

Data Controller(s)	NHS Sheffield 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	<p>Article 6 – 6(1)(c) ‘...necessary for compliance with a legal obligation...’</p> <p>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.</p> <p>Relevant legislation: the provisions of the Safeguarding Vulnerable Groups Act 2006 as a basis for carrying our DBS checks.</p>
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, the names of those being interviewed will be provided to the interview panel. On occasion the interview panel may include colleagues external to the CCG, such as the Local Authority. 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	Methods Consulting Ltd – management of NHS Jobs (recruitment website)
Your Rights	<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 be notified of data breaches
How long we will keep the information	For unsuccessful job applicants, information is retained for 1 year. For successful applicants, job application information is retained for 3 years.
Who we will share the information with (recipients)	This information is not usually shared outside of the CCG unless an individual external to the CCG is included on the interview panel.

Human Resources

Data Controller(s)	NHS Sheffield CCG NHS Business Services Authority (for the Electronic Staff Record aspect)
Purpose	The CCG holds personal and confidential information if 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	<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 employment...social protection law in so far as it is authorised by Union or Member State law.</p> <p>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.</p> <p>Relevant legislation: the provisions of the Safeguarding Vulnerable Groups Act 2006 as a basis for carrying our DBS checks.</p>
How we collect (the source) and use the information	<p>The CCG uses information for the purposes of employment in a variety of ways including:</p> <ul style="list-style-type: none"> • Recruitment – application forms, collecting references, carrying out DBS checks, payroll and pension information.

	<ul style="list-style-type: none"> • Managing and monitoring annual leave and sickness. • Carrying our personal development reviews. • Referrals to Occupational Health • Disciplinary procedures. • Processing staff leavers, retirements and providing references. • Recruitment of temporary staff/student placements
Data Processors	<p>Victoria Pay Services (Payroll) NHS Sheffield Teaching Hospitals IBM (system supplier of the Electronic Staff Record - ESR) Methods Consulting Ltd – management of NHS Jobs (recruitment website) NHS SBS (finance system) for payroll purposes Health Management Limited – provider of Occupational Health services</p>
Your Rights	<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 be notified of data breaches
How long we will keep the information	In accordance with the Records Management Code of Practice for Health and Social Care 2016
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> <ul style="list-style-type: none"> • Public disclosure under Freedom of Information - e.g. requested names or contact details of senior managers or those in public-facing roles; • Disclosure of job applicant details - e.g. to named referees for reference checks, to the Disclosure & Barring Service for criminal record checks • Disclosure to employment agencies - e.g. in respect of agency staff; • Disclosure to banks & insurance companies - e.g. to confirm employment details in respect of loan/mortgage applications/guarantees; • Disclosure to professional registration organisations - e.g. in respect of fitness to practice hearings; • Disclosure to Occupational Health professionals (subject to explicit consent); • Disclosure to police or fraud investigators - e.g. in respect of investigations into incidents, allegations or enquiries.

Declarations of Interests, Gifts and Hospitality Publication

Data Controller(s)	NHS Sheffield 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)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

	<p>authority</p> <p>Statutory guidance for CCGs on Managing Conflicts of Interest under Section 14O of the National Health Service Act 2006 (as amended by the Health and Social Care Act 2012)</p>
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	None
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	The CCG will keep 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)	The registers are published on the CCG's website. Information may be shared with NHS England.

National Fraud Initiative

Data Controller(s)	NHS Sheffield 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. 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>
Data Processors	None
Your Rights	<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 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

Glossary

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

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

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

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

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

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 (eg Law Enforcement). This Act will repeal the UK Data Protection Act 1998.

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.

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.

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.

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

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

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

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.

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.

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.

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.