

OFFICIAL

FAIR PROCESSING NOTICE

NHS Sunderland Clinical Commissioning Group

NHS Sunderland Clinical Commissioning Group
Pemberton House
Colima Avenue
Sunderland Enterprise Park
Sunderland
SR5 3XB

Telephone: 0191 512 8484

Email: SUNCCG.sccg@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 [here](#). 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.

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](#) – such requests are processed by North of England Commissioning Support Unit on our behalf and explicit patient consent is sought to enable us to do this assessments for [continuing healthcare](#) (a package of care for those with complex medical needs) and appeals - – such requests are processed by North of England Commissioning Support Unit on our behalf and explicit patient consent is sought to enable us to do this

OFFICIAL

- responding to your [queries, compliments or concerns](#) - such requests are processed by North of England Commissioning Support Unit on our behalf and explicit patient consent is sought to enable us to do this
- 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).
- 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](#)

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/>

Type 2 objections are 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.

Fair Processing Notice

Sunderland CCG

May 2018

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 <mailto:NECSU.IG@nhs.net>

The DPO for our member practices is James Carroll, who can be contacted via email at DPO.SUNCCG@NHS.NET or via telephone on 0191 404 1000 Ext 3436.

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.

OFFICIAL

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).

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 Dr Claire Bradford, 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 Scott Watson, Director of Contracting and Business Intelligence. 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

In some instances, you are allowed to request that your confidential information is not used beyond your own care and treatment and to have your objections considered. To support this patients are able to register objections with their general practice to either prevent their identifiable data being released outside of the GP Practice (known as a Type 1 objection) or to prevent their identifiable data from any health and social care setting being released by NHS Digital (known as a Type 2 objection) where in either case it is for purposes other than direct patient care. 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.

NHS Digital is developing a new system to support the national data opt-out which will give patients more control over how their personally identifiable data is used. The system will let patients exercise their right to make an informed choice about whether their personally identifiable data is only used for their individual care and treatment or also shared for research and planning purposes. Further information regarding opting out is available from the NHS Digital website here <https://digital.nhs.uk/national-data-opt-out>

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 [here](#)

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. This Fair Processing notice was last updated in January 2018.