

Fair Processing Notice - How Use Your Information

This notice is designed to inform you of the type of information (including personal information) that we NHS Lewisham CCG, as your clinical commissioning group (CCG), holds about you, how that information is used, who we may share that information with, and how we keep it secure and confidential.

What we do

We Lewisham CCG are responsible for planning, buying and monitoring (also known as commissioning) health services from healthcare providers, such as 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.

How we use your information

We hold some information about you and this document outlines how that information is used, who we may share that information with, how we keep it secure (confidential) and what your rights are in relation to this. Your records are used to direct and manage the care you receive to ensure that healthcare professionals have the information they need to be able to assess and improve the quality and type of care you receive, and so that your concerns can be properly investigated if a complaint is raised.

These uses are in line with the purposes outlined in our registration with the Information Commissioners Office and the reference number is ZA014148.

What are Primary Care Data and Secondary Care Data?

As many people's first point of contact with the NHS, around 90 per cent of patient interaction is with primary care services. In addition to GP practices, primary care covers dental practices, community pharmacies and high street optometrists. Primary Care Data relates to information which has been sourced from these types of services.

Secondary Care covers treatment and care of a specialised medical service by Clinicians, for example, specialist doctors and nurses, within a health facility or hospital on referral by a primary care clinician (e.g. your GP). Secondary Care data relates to information which have been sourced from these types of services.

The Secondary Uses Service (SUS) is the single, comprehensive repository for healthcare data in England which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. When a patient or service user is treated or cared for, information is collected which supports their treatment. For further information, please visit NHS Digital's website: <http://digital.nhs.uk/sus>

SUS data useful to commissioners and providers of NHS-funded care for 'secondary' purposes - purposes other than direct or 'primary' clinical care, as we have stated previously like how the CCG uses information. We go into more detail within the '**Do you share my information with other organisations**' section below.

What kind of information do we use?

We use six types of information/data:

1. Anonymised data, which is data about you but from which you cannot be personally identified;
2. De-identified data with pseudonym identifier, which is data about you but we are able to track you through the patient pathway without using your personal information, and you cannot be personally identified;
3. De-identified data with weakly pseudonym identifier such as the NHS number. We use this to link two or more types of datasets together using your NHS number. For example, using your NHS number to link and analyse datasets such as acute data with community data to see the full picture of your patient pathway. No other personal information is used during this process and you will not be personally identified. However, there may be times whereby you may be re-identified in the event of patient safety requirements, or re-identified for direct care purposes where we pass on information to your GP to treat you;
4. Anonymised in Context (for commissioning purposes), which is de-identified data about you but from which you cannot be personally identified within a commissioning (CCG) environment. You may be personally identified if this data was available to a hospital or your GP. Like the above, we replace the NHS number with a locally generated pseudonym like hospital number;
5. Personal data from which you can be personally identified; and
6. Sensitive information/data about you from which you can be identified.

What do we use these types of data for?

We use the above types of data to plan health care 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; and
- Review the care being provided to make sure it is of the highest standard.

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. A full list of services can be found on our [services' page](#). We may also share anonymised statistical information with them for the purpose of improving local services: for example, understanding how health conditions spread across our local area compared to other areas.

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

Data may be linked and de-identified by these special bodies so that it can be used to improve health care and development, and monitor NHS performance. Where data is used for these statistical purposes, stringent measures are taken to ensure individual patients cannot be identified.

When analysing current health services and proposals for developing future services, it is sometimes necessary to link separate individual datasets to be able to produce a comprehensive evaluation. This may involve linking primary care GP data with secondary care, 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 and audiology, as well as mental health and community-based services such as IAPT, district nursing and podiatry. When carrying out this analysis, the linking of these datasets is always done using a pseudonym as the CCG does not have access to patient identifiable data.

The following are the types of organisations HSCIC (NHS Digital) receives data from, and then forwards on to our data processor in a de-identified format or a dataset with a weakly pseudonym identifier (NHS Number) format to link and analysis the data.

Types of organisations and types of information we receive:

- Acute Trusts – Hospitals, for example Guys and St Thomas' NHS Trust, Kings College NHS Foundation Trust, Lewisham and Lewisham NHS Trust We receive pseudonymised acute data such as A&E attendances, waiting times, diagnosis, treatments, and follow ups, length of stay, discharge information and next steps.
- Community trusts or community organisations such as Oxleas NHS Foundation Trust, Bromley Healthcare and Greenwich & Lewisham NHS Trust. We receive pseudonymised community data such as outpatient information, waiting times, diagnosis and treatments, referrals and next steps, domiciliary and district nursing (which includes home visits) and community rehabilitation units.
- Mental Health Trusts or Mental Health organisations such as Oxleas NHS Foundation Trust and South London & Maudsley NHS Foundation Trust. We receive pseudonymised mental health data such as rehabilitation and outpatient attendances, waiting times, diagnosis, treatment, length of stay, discharge, referrals and next steps.
- Primary Care organisations, for example your local GP practice. We receive pseudonymised primary care data such as attendances, diagnosis, treatment, GP or GP practice visits, referrals, medication/prescriptions information, follow-ups and next steps.

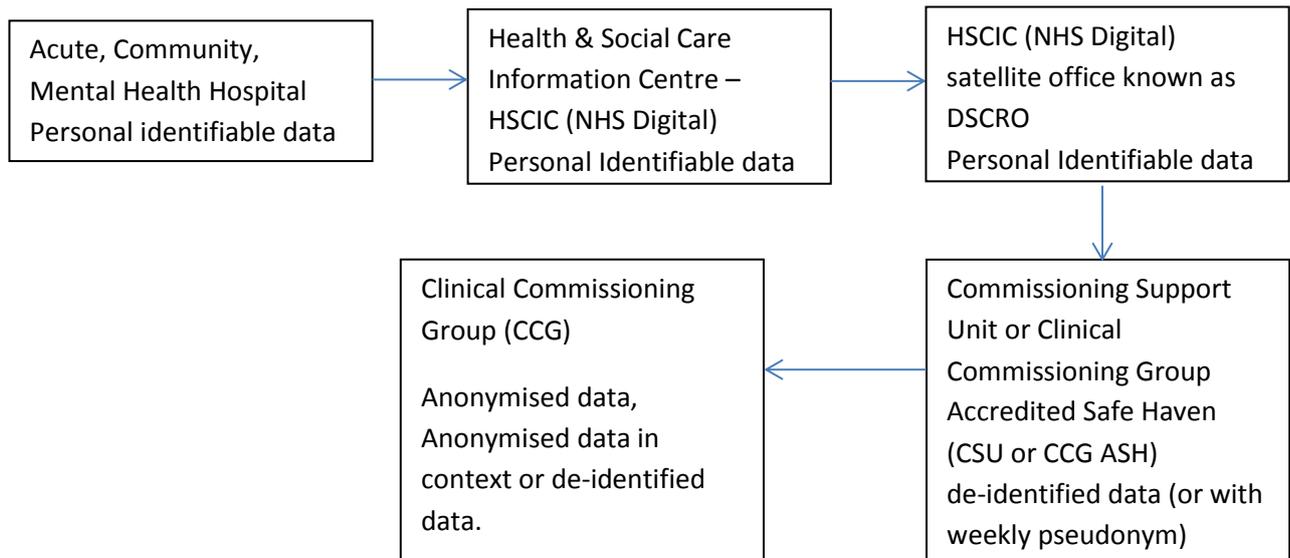
It is also important to note that if you receive treatment in another part of the country, for example if you are on holiday, HSCIC (NHS Digital) will receive information about your treatment. We will receive this information in a de-identified dataset in accordance with point 2 and 3 above within the '**what kind of information do we use**', as it's important to link and analyse your patient pathway.

We may also contract with other organisations to process data. We ensure external data processors that support us are legally and contractually bound to operate this process. They must be able to prove security arrangements are in place where data that could or does identify a person is processed.

Currently, the external data processors we work with include (amongst others):

- NHS South East Commissioning Support Unit

This is how all the above processing works:



Invoice Validation

There may be times where one healthcare organisation will need to invoice another for treatment given to a patient. This can occur, for example, when you need hospital treatment while away from home on holiday. The hospital at which you were seen may need to invoice us for the treatment you received.

Before paying the invoice, we will need to be sure that we are responsible for your treatment costs and not another CCG, as well as checking to ensure that the amount you are being billed for is correct. This process is known as invoice validation. For invoice validation to occur, a limited amount of information about you needs to be shared between us and the hospital where you received treatment. The following table outlines type of information we may share and justification for use of this information.

Lewisham CCG uses the services of a health partner, NHS South East Commissioning Support Unit (South East CSU) to process this data on our behalf to enable the appropriate payment to be processed. South East CSU does not use any information from NHS Digital for this process, the information is provided directly from where you received the treatment. Once the invoice has been paid, the limited information about you is deleted, as it is no longer required. If the information is needed again, to respond to a question, it will be requested, the question answered and the information deleted again.

Clinical Commissioning, opens in new window Groups (CCGs) and Definition of: Commissioning, opens in new window Support Units (CSUs) have received approval under Regulation 5 of the Health Service (Control of Patient Information) Regulations 20021 to process patient identifiable information without Definition of: consent, opens in new window for the purposes of invoice validation. This approval provides the legal basis for Health Service Definition of: Providers, opens in new window to disclose patient Definition of: confidential, opens in new window information to named organisations for the purposes of invoice validation.

NHS LewishamCCG, has the correct safeguards in place and are recorded on the NHS England register of CEfF's: <http://www.england.nhs.uk/wp-content/uploads/2014/07/ceff-app-orgs.pdf>

Further information regarding CEfF and Invoice validation can be found on the NHS England Website: <http://www.england.nhs.uk/ourwork/tsd/ig/in-val/>

The information we might need as part of invoice validation is outlined below with examples and justification for use of each type of information item.

Information Type	Example	Purpose	Justification
Invoice Number	Not PCD	Identifies the relevant invoice and allows associated with backing data	To enable backing data to be matched with the relevant invoice
NHS Number	NHS Number	The unique identifier for the patient	Needed to determine if the individual is the responsibility of the CCG
Unique Patient Event identifier	Hospital Provider Spell Number/AE or OP Attendance identifier unique within Provider for the patient event	To ensure the same episode of care isn't paid for by the commissioner more than once. For example, a patient may have several attendances of treatment on the same day.	To distinguish between multiple events carried out for a particular patient on the same day.
Unique Patient Identifier	Local Patient Identifier, GP Practice identifier	To ensure any issue or payment is attributed to the same patient	To identify the individual to the healthcare provider. Particularly as NHS Number is not always known by the provider.

Handling Continuing Healthcare (CHC) Applications

If you make an application for Continuing Healthcare (CHC) funding, Lewisham CCG will use the information you provide and where needed request further information from care providers to identify eligibility for funding. If agreed, arrangements will be put in place to arrange and pay for the agreed funding packages with appointed care providers. This process is nationally defined and we follow a standard process and LEWISHAM CCG - use standard information collection tools to decide whether someone is eligible.

Handling Individual Funding Requests (IFR) Applications

If you make an Individual Funding Request (IFR) to fund specialist drugs or rare treatments, LEWISHAM CCG will use the information you provide and where needed request further information from care providers to identify eligibility for funding. If agreed, arrangements will be put in place to arrange and pay for the agreed funding packages with appointed care providers.

Supporting Medicines Management

CCGs support local GP practices with prescribing queries which generally don't require identifiable information.

Where specialist support is required, e.g., to order a drug that comes in solid form in gas or liquid the medicines management team will order this on behalf of a GP to support your care.

Safeguarding

Advice and guidance is provided to care providers to ensure that adult and children's safeguarding matters are managed appropriately. Access to identifiable information will be shared in some limited circumstances where it's legally required for the safety of the individuals concerned.

Quality Alerts

A Quality Alert is a systemic issue, generally affecting a service, or the ability to deliver a high quality service. LEWISHAM CCG's Governance and Quality Team triage quality alerts (QA's) reverse quality alerts and incidents reported by GPs/Provider organisations. The CCG has a statutory duty to support NHSE with the continuous quality improvement of primary medical services as set out in the HSCA 2012 and the Primary Medical Services assurance framework. For the CCG to triage quality alerts and incidents reported by Lewisham GPs and providers, the Governance and Quality team at the CCG may require the relevant individual's NHS number in order to investigate the quality alert or incident.

Post Infection Reviews

Clinical Commissioning Groups collaborate 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.

CCGs will lead the Post Infection Review in the circumstances set out in the Post Infection Review Guidance, issued by NHS England. They will be able to use the results of the Post Infection Review to inform the mandatory healthcare associated infections reporting system.

Serious Incident Management

LEWISHAM CCG is accountable for effective governance and learning following all Serious Incidents (SIs) and work closely with all provider organisations as well as commissioning staff members to ensure all SIs are reported and managed appropriately. The Francis Report (February 2013) emphasised that commissioners,

as well as providers had a responsibility for ensuring the quality of health services provided.

Sharing Information

In order for LEWISHAM CCG to perform its commissioning functions, information (mostly anonymised) is shared from various organisations which include: General practices, acute and mental health hospitals, other CCGs, community services, walk-in centres, nursing homes, directly from service users and many others.

Risk stratification

Your GP uses your data to provide the best care they can for you. As part of this process, your GP will use your personal and health data to undertake risk stratification, also known as case finding.

Risk stratification involves applying computer based algorithms, or calculations, to identify those patients registered with the GP Surgery who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition.

To identify those patients individually from the patient community registered with your GP would be a lengthy and time-consuming process, which would by its nature potentially not identify individuals quickly and increase the time to improve care.

Your GP Surgery uses the services of a health partner, NHS South East Commissioning Support Unit (South East CSU) to identify those most in need of preventative or improved care. This contract is arranged by us.

Neither we nor NHS South East CSU will at any time have access to your personal or confidential data. They act on behalf of your GP to organise this service with appropriate contractual and security measures only.

South East CSU will automatically process your personal and confidential data without any staff being able to view the data. Typically they will process your data using indicators such as your age, gender, NHS number and codes for your medical health to identify those who will benefit from clinical intervention.

Processing takes place automatically and without human or manual handling. Data is extracted from your GP computer system, automatically processed, and only your GP is able to view the outcome, matching results against patients on their system.

We have implemented strict security controls to protect your confidentiality and recommend this as a secure and beneficial service to you. At all times, your GP remains accountable for how your data is processed. However, if you wish, you can ask your GP for your data not to be processed for this purpose and your GP will mark your record as not to be extracted so it is not sent to South East CSU for risk stratification purposes.

The lawful basis to use this information for risk stratification has been allowed by s251 NHS Act 2006 and is processed by South East CSU or other approved providers only. For further information on Risk Stratification, please visit <https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/> and <http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/>

Caldicott Guardian

Each NHS organisation and General Practice is required by mandate to have a Caldicott Guardian who has responsibility for satisfying the highest practical standards for handling patient identifiable, confidential and sensitive information. The Caldicott Guardian also actively supports work to enable information sharing where it is appropriate and advises on options for lawful and ethical processing of patient information.

How you can access your records

The Data Protection Act 1998 gives you a right to access the information we hold about you on our records. Requests must be made in writing to:

Information Governance Team
South East Commissioning Support Unit
3rd Floor, 1 Lower Marsh,
London
SE1 7NT

You can email: SECSU.InformationGovernance@nhs.net

We will reply to your request within 40 days from receipt and in order to provide the correct information we will need:

- Your personal details including your full name, address, date of birth, and NHS number so that your identity can be verified and your records located
- A cheque for an initial £10 (rising to a maximum of £50 for health records) made payable to NHS Lewisham Clinical Commissioning Group
- An indication of what information you are requesting to enable the CCG to locate this in an efficient manner

For independent advice about data protection, privacy and data-sharing issues, you can contact the;

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
CheshireSK9 5AF
Phone: 08456 30 60 60 or 01625 54 57 45
Website: www.ico.org.uk

Managing conflicts of interest

We manage conflicts of interest as part of our day-to-day activities. Effective handling of conflicts of interest is crucial to give confidence to patients, tax payers,

healthcare providers and parliament that CCG commissioning decisions are robust, fair, transparent and offer value for money. It is essential in order to protect healthcare professionals and maintain public trust in the NHS. Failure to manage conflicts of interest could lead to legal challenge and even criminal action in the event of fraud, bribery and corruption.

Section 14O of the National Health Service Act 2006 (as amended by the Health and Social Care Act 2012) (“the Act”) sets out the minimum requirements of what both NHS England and CCGs must do in terms of managing conflicts of interest.

Any persons who are included in the declaration of interest registers can contact the Data Protection Officers for the NHS **Lewisham CCG** at;

South East Commissioning Support Unit

3rd Floor, 1 Lower Marsh,

London

SE1 7NT

You can also email: SECSU.InformationGovernance@nhs.net

Patient right to object to processing/opt-out

There are choices you can make about how your information is used, and you can choose to opt out of your information being shared or used for any purpose beyond providing your care.

If you do not want your information to be used for any purpose 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.

There are two types of opt-out. You can withdraw either opt-out at any time by informing your GP practice.

Type 1 opt-outs

If you do not want information that identifies you to be shared outside your GP practice, for purposes beyond your direct care, you can register a type 1 opt-out with your GP practice. This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Type 2 opt-outs

The HSCIC collects information from a range of places where people receive care, such as hospitals and community services. If you do not want your personal confidential information to be shared outside of the HSCIC, for purposes other than for your direct care, you can register a type 2 opt-out with your GP practice.

A [direction](#) from Secretary of State sets out the Department of Health policy as to how type 2 opt-outs must be applied and instructs NHS Digital (HSCIC) to apply type 2 opt-outs from 29 April 2016.

When we have collected information about your type 2 opt-out from your GP practice we use that to create a record of all current type 2 opt-outs. We then use that record to check against any set of data that is to be made available by NHS Digital (HSCIC) to another organisation and remove all of your personal confidential information if it is in that data set, before that data are made available.

The direction sets out the scope of when your type 2 opt-out does not apply, such as when there is a legal requirement to release information, or where you have given your consent to a specific release of your information.

There are also some limited circumstances, which are set out in the direction, when we don't apply your type 2 opt-out to information made available. These are cases where:

- The Secretary of State for health has identified the information flow is very important.
- There are complex technical barriers that make it very difficult to apply opt-outs.

For more information on how we collect and use opt-out information see [Applying Type 2 Opt Outs](#)

For more information about care records and how to access them see NHS Choices at the following link

<http://www.nhs.uk/NHSEngland/thenhs/records/healthrecords/Pages/overview.aspx>.

For details about how public bodies must make information available, see the model publication scheme published by the Information Commissioner's Office.

<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/publication-scheme/>

How long we will keep your information and how we will destroy information

There are different retention schedules for different types of information and types of record. In the NHS, all commissioners and providers apply retention schedules in accordance with the Information Governance Alliance's Records Management Code of Practice for Health and Social Care. For more information, you can access the document here: <http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf>

NHS data are subject to legal retention periods and should not be destroyed unless specific instructions to do so has been determined and received from the Data Controller. Where data has been identified for disposal:

- NHS organisations have the responsibility to ensure that NHS information held in manual form (regardless of whether originally or printed from the IT systems) is destroyed using a cross cut shredder or subcontracted to a reputable confidential waste company that complies with European Standard EN15713.

- NHS organisations also ensure that electronic storage media used to hold or process NHS Information is destroyed or overwritten to current CESC standards as defined at www.cesg.gov.uk. NHS ICT Teams usually carry out or contract out to an approved company to ensure the secure destruction or permanently removal of information from ICT equipment which are NHS assets. In the event of any bad or unusable sectors that cannot be overwritten, the NHS ICT Team or approved contractor shall ensure complete and irretrievable destruction of the media itself.
- It is the responsibility of NHS organisations to retain copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the contract.

Any arrangement made by NHS organisations to sub-contract secure disposal services from another provider, must comply with clause GC 12 of the NHS Standard Contract and with assurance that the sub-contractor's organisational and technical security measures comply with the 7th Data Protection Act 1998 principle

Compliance

Your care provider and CCG will endeavour at all times to comply with the statutory duties, laws and NHS policy which govern their use of personal and confidential information. These include the following:

- [The NHS Constitution;](#)
- [The Care Records Guarantee;](#)
- [Data Protection Act 1998;](#)
- [Health and Social Care Act 2012;](#)
- [Freedom of Information Act 2000;](#)
- [Children's Act 2004;](#)
- [NHS Confidentiality Code of Conduct;](#)
- [Common Law Duty of Confidentiality;](#)
- [Access to Health Records Act 1990.](#)
- [Health Research Authority](#)