NHS
Ealing
Clinical Commissioning Group

Fair processing notice

This notice is intended to inform you about the type of patient information that NHS Central London CCG holds, how that information might be used, with whom we may share that information, and how we ensure it is kept secure.

What we do

NHS Ealing CCG is responsible for planning and designing local health services. In order to do this, we buy (commission) health care services including:

• Planned hospital care

• Urgent and emergency care

• Rehabilitation care

• Community health services

• Mental health and learning disability services

We regularly monitor the performance of these services, and through our Complaints team we deal with any concerns raised by patients with services we directly commission.

We work with key stakeholders such as local health and social care providers, patient groups and local community groups to ensure the services we commission meet local needs.

Why we collect personal information

In order for us to ensure that the services we commission are meeting patients' needs, we may collect information about the patients using these services.

Examples of identifiable data we may hold are:

• Name

• Address

• Postcode

• Date of Birth

• NHS Number

The CCG is the data controller. This means that the CCG determines the purposed for which and the manner in which any personal data are, or are to be, processed. The CCG processes information made by patients regarding concerns they have relating to care provided by services we commission. We work collaboratively with our care provider organisations, and patients to ensure that all complaints made are appropriately investigated

In addition, we may also process personal data to validate invoices from service providers relating to patients within our locality and also risk stratification purposes.

Provider organisations from outside of our local area will send invoices for the care they have provided to our patients, as this ad hoc care provision is not covered by the contracts we manage locally. As such, there is a requirement for the CCG to be sent supporting personal identifiable information in order to validate the invoices.

Risk stratification enables GPs, supported by the CCG, to target specific patient groups and enable clinicians, with the duty of care for the patient, to offer appropriate interventions. The long term aim is that patients with particular care needs can be identified early and treated on a more personalised basis.

More information on these potential uses can be found via the links below:

https://www.england.nhs.uk/ourwork/tsd/ig/in-val/

https://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/

How we use patient information

We may share information with, or receive information from, other NHS and partner organisations for the purposes of commissioning local services. This information sharing helps the CCG ensure that we are providing the services

Whilst the majority of the information we hold is anonymised, the CCG also process data in personal identifiable and pseudonymised formats.

We may also hold other personal data relating to complaints, investigations, individual funding requests, continuing healthcare funding, or reviews that we carry out on behalf of patients or in collaboration with partner organisations.

This data is generally used to help us plan the commissioning of healthcare services. This includes:

• Evaluating and reviewing the quality and efficiency of services we commission

• Forecasting local healthcare need to ensure that the demands for services are met where appropriate and necessary

• Benchmarking our service delivery and commissioning locally and nationally

We access the Commissioning Data Set, which is the consistent format used for the submission of commissioning data to the Secondary Uses Service for outpatient and A&E attendances, critical care activity, admitted patient care and elective admission list data. This information is essential to the CCG being able to work with providers, and ensure that the services we commission are reflective of the needs of our local health communities.

In some instances, we will link different datasets in order to obtain a more holistic picture of the local community. For example as part of the Whole Systems Integrated Care Record, we link data from primary and secondary care in order to provide an integrated care record that in time, will be accessible to staff in primary, secondary and social care settings.

For the CCG to process personal information, for the provision of indirect care, we make use of a number of nationally approved secure systems and processes to facilitate the transfer of data. This includes, but is not limited to:

Accredited Safe Haven (ASH) – The ASH in North West London is hosted by NHS Brent CCG on behalf of the Health and Social Care Information Centre (HSCIC). The ASH allows patient identifiable data to flow in from various data sources and then reproduce that data in either a pseudonymised or anonymised format to be used for commissioning and other purposes. One of the pre-requisite requirements for obtaining ASH status is being compliant with the Information Governance Toolkit by having a 'satisfactory' toolkit submission.

Data Services for Commissioners Regional Offices (DSCRO) – This is a secure facility provided by the South East Commissioning Support Unit (SECSU) on behalf of the HSCIC. More information about the DSCRO service can be found here: http://www.hscic.gov.uk/dataservicesforcommissioners

Controlled Environment for Finance – This service is hosted by NHS Brent CCG on behalf of NHS England to support Invoice Validation. This service was established to allow commissioning organisations to validate invoices it receives, ensuring correct payments are identified and made on behalf of the CCG with section 251 support. This allows the transfer of data from the HSCIC to commissioning organisation Accredited Safe Havens for explicitly listed purposes, one of which is invoice validation.

Each of these information uses are in line with the purposes outlined in our registration with the Information Commissioners Office.

Key definitions:

Personal data is defined within the Data Protection Act 1998 as "data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller"

Sensitive personal data is defined in section 2 of the Data Protection Act as personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Anoymised data is data that has been had all unique identifiers removed. The removal of identifiers means that individuals can no longer be identified from the data.

Pseudonymised data takes data fields with identifiable data and replaces them with artificial identifiers, or pseudonyms. For example a name is replaced with a unique number. The purpose is to render the data record less identifiable, whilst still retaining the usefulness and ability to re-identify individuals where necessary.

Direct patient care is defined within the Caldicott Review as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of

individuals. It includes supporting individuals' ability to function and improve their participation in life and society.

Indirect patient care is defined within the Caldicott Review as activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care.

Explicit Consent occurs when a patient specifies the particular types of data they wish to be shared about them and the specific purposes for which the data may be used.

Implied Consent occurs when explicit consent has not been obtained, and instead consent is not expressly granted by a person, but rather implicitly granted, or inferred, by a person's actions and the facts and circumstances of a particular situation (or in some cases, by a person's silence or inaction).

Primary care data is considered to be data obtained from a range of primary care services such as GPs, dentists and community pharmacies.

Secondary care data is data from the secondary care sector, which includes acute NHS providers, community providers and mental health trusts.

Data controllers are the people who (either alone or jointly or in common with other persons) determine the purposes for which, and the manner in which, any personal data are, or are to be, processed.

A data processor is any person (other than an employee of the Data Controller) who processes data on behalf of the Data Controller. Through their ASH and DSCRO statuses, NHS Brent CCG and SECSU act as data processors on behalf of the CCG.

How we keep information confidential

We process and manage information in accordance with our legal duties under the Data Protection Act 1998. This includes the requirement to keep information secure and not hold it for longer than necessary.

To support our legal duties, the CCG has a robust suite of Information Governance policies in place, including policies on information security, confidentiality and data protection. The CCG follows the retention and destruction guidelines issued in the Records Management Code of Practice. https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Under the Data Protection Act, we must ensure we have a legal justification for holding and using personal information. Under the Common Law Duty of Confidentiality, we have a duty to respect any duty of confidence attached to information we hold.

As an NHS organisation, we work in accordance with the confidentiality principles and guidelines laid out in the Caldicott reviews and the ‘Confidentiality: NHS Code of Conduct’.

We have strict information governance terms and conditions within our contractual agreements and policies and procedures which outline the expectations we have on staff to safeguard personal information. We ensure that all staff who access personal information receive appropriate on-going information governance training.

How to access information held about you by the CCG

If you wish to request a copy of information held about you, please do so by writing to the CCG:

Information Governance Lead

Central London CCG

15 Marylebone Road

London

NW1 5JD

Under the Data Protection Act 1998 you have the right to see or be given a copy of personal data held about you. To gain access to your information you will need to make a Subject Access Request (SAR)

We may charge a reasonable fee for the administration of the request, set down in law as follows:

• If the information is only held electronically we may charge up to £10 for complying

• If the information is only held wholly or partly in paper format we may charge up to £50 for complying.

NHS England has published information on their website for patients about the different ways to obtain information held by NHS organisations.

How to Opt Out:

If you wish to opt out of having your personal data shared please contact your GP in the first instance as local and national information sharing initiatives are derived from the GP record in the primary instance.

There are two different types of objection which both refer to information sharing for purposes other than that of direct patient care:

Type 1 objections occur when a patient objects to their GP about having their identifiable data shared outside of their GP practice.

Type 2 objections occur when a patient objects to their identifiable data being disclosed to the HSCIC.

The HSCIC monitors the number of patients applying their type 1 and 2 rights through aggregated data sources.

Whilst patients have the right to opt out of having their data shared for purposes other than direct patient care, sharing data allows the NHS to better understand the needs of patients. It also allows for more comprehensive performance monitoring of services and allows organisations to adequately benchmark themselves. This allows care providers and commissioners to work collaboratively to improve the quality of, and accessibility to, local services.

There are some instances where patients cannot opt out of having their information shared and information may be shared without explicit or implied consent. These instances may include:

• Where there are sufficient safeguarding or vulnerability concerns

• There is an overriding public interest in releasing or sharing information

• Where the sharing is mandated by law or court order.

If you have any concerns or queries regarding this, please contact your GP in the first instance although you can contact the CCG's Information Governance Team:

Information Governance Lead

Central London CCG

15 Marylebone Road

London

NW1 5JD

Other useful links:
The following links and documents encompass various local and national information sharing initiatives as well as links to patient forums

NHS Care Records Guarantee - http://systems.digital.nhs.uk/rasmartcards/documents/crg.pdf

The NHS Constitution -
https://www.gov.uk/government/publications/the-nhs-constitution-for-england

North West London Whole Systems Integrated Care Record -
http://integration.healthiernorthwestlondon.nhs.uk/

Health and Social Care Information Centre (HSCIC) Guide to Confidentiality -
http://digital.nhs.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

Health Research Authority - http://www.hra.nhs.uk/

Further information

If you have any questions or concerns regarding the patient information we may hold about you, or how we use this information, there are a number of ways you can raise contact us to discuss:

You may use the contact us link on our website.

Alternatively, you can write to the CCG's Caldicott Guardian:

Director of Nursing and Quality

15 Marylebone Road

Information Governance Lead

15 Marylebone Road

London

NW1 5JD

The Caldicott Guardian is responsible for championing confidentiality and patient's information rights at an executive level within the CCG.