

Privacy notice

Contents

How we use your data.....	2
What we do.....	2
Why we hold information about you.....	2
Keeping information secure and confidential.....	3
How information is used.....	3
Definition of data types.....	4
What is primary care data and secondary care data?.....	5
Data linking.....	5
NHS Digital.....	6
Data processors.....	7
Invoice validation.....	8
Risk stratification.....	8
Information sharing with non-NHS organisations.....	9
Patient rights.....	10
Type 1 opt-out.....	11
Type 2 opt - out.....	11
How long we will keep your information and how we will destroy information.....	12
How you can get access to your records?.....	12
Caldicott Guardian and Senior Information Risk Owner (SIRO).....	13
Employee information.....	13
Managing conflicts of interest.....	14
Questions or concerns.....	14
Changes to this privacy notice.....	15
Contact the Information Governance team.....	15

How we use your data

What we do

NHS Kernow Clinical Commissioning Group (NHS Kernow) is 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.

The purpose of this notice is to inform you of the type of information (including personal information*) that NHS Kernow holds, how that information is used, who the information may be shared with, how it is kept secure and confidential and what your rights are in relation to this.

*Personal information data is data which relates to a living individual who can be identified:

- a) From that data.
- b) From that data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Why we hold information about you

The purpose of gathering the information is: to make sure funding for health and care services is targeted where it is needed the most, to ensure appropriate care and treatment is provided where and when it is needed, is of the highest standards and ultimately, local people are able to lead longer, healthier lives. For example, services are commissioned or provided from hospitals, community health services, general practitioners (GPs) and dentists.

You can read more about each of these roles by visiting the websites for those organisations or selecting the internet links which are contained within this Privacy Notice.

The collection of accurate information about you is vital in assisting your GP, primary care team and NHS Kernow in providing you with the right services and health care for your needs. This enables you to be given appropriate information about your care, to make informed choices and where possible improve the services you receive.

Records may be electronic, paper or a mixture of both and may be used in combination or separately, with working practices and technology to ensure that your information is kept confidential and secure.

All health and social care organisations and their staff are committed to protecting your privacy, will only use information collected lawfully in accordance with the Data Protection Act 2018 and undertake not to use any information held about you for any purpose other than that for which it was collected, unless your consent has been obtained.

Keeping information secure and confidential

All staff have contractual obligations of confidentiality, enforceable through disciplinary procedures. Staff with access to patient identifiable information have received appropriate on-going information governance training to ensure they are aware of their responsibilities and staff are only granted access to personal data on a need-to-know basis only.

We also have to honour any duty of confidence attached to information and apply Common Law Duty of Confidentiality requirements. This will mean where a legal basis does not exist to use your personal or confidential information we will not do so.

NHS Kernow also abides by the General Data Protection Regulations (GDPR) which enables the sharing of personal information, where appropriate, with other European Union countries. In addition, information collected will not be sent to any other countries where the laws do not protect your privacy to the same extent as that required by GDPR. Unless required to do so by law, your information will not otherwise be shared, sold or distributed to any third party without your consent.

The Care Record Guarantee is our commitment that all NHS organisations and those providing care on behalf of the NHS will use records and information about you in ways that respect your rights and promote your health and wellbeing. Everyone who works for the NHS or for organisations delivering services under contract to the NHS must comply with this guarantee.

We make sure the information we hold is stored securely and access to it is restricted to authorised personnel. We have organisational and technical security in place to protect personal and confidential information, for example using encrypted laptops and being especially carefully with disposal of items, like paperwork, computer disks and memory sticks.

How information is used

We use the following types of information/data:

- Identifiable: containing details that identify individuals.
- Pseudonymised: about individuals but with identifying details (such as name or NHS number) replaced with a unique code.
- Anonymised: about individuals but with identifying details removed.
- Aggregated: anonymised information grouped together so that it doesn't identify individuals.

Definition of data types

This section provides definitions for key terms which are used throughout this text to describe different data types.

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

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.

De-identified data with weak 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.

Anonymised in context data (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 an information system number.

Anonymised statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units, and research institutions to help with future development of services.

Examples of how this information is used:

- Working out what illnesses people will have in the future so we can all work with the local primary care services, community services and hospital services to ensure that patient needs are met now and in the future.
- Planned hospital care.
- Rehabilitation care.
- Some mental health and learning disability services.
- Responding to patient concerns about services.

- Checking accounts and services.
- Audit and public health services.

We use anonymised 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.

Some of the areas where personal information will be used are:

- To provide direct patient care.
- Referral management processes – to ensure you are referred to the right service when requested by your GP.
- Individual Funding Requests - a process where patients and their GPs or consultants can request special treatments not routinely funded by the NHS.
- Continuing healthcare assessments (a package of care for those with complex medical needs).
- Responding to your queries, concerns or complaints.
- Assessment and evaluation of safeguarding concerns for individuals.
- Incident investigations.
- Where there is an overriding public interest.
- Where we have gathered your consent.
- Where there is a legal requirement for us to do so.

NHS Kernow also processes personal information in relation to the staff it employs (and contractors it works with). Further information regarding the confidentiality of staff information can be found towards the end of this Privacy Notice.

What is primary care data and secondary care data?

Around 90 per cent of people's contact with the NHS is with primary care services. These include services such as those provided by GP practices, 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 the treatment and care provided by specialised medical services. These include specialist doctors and nurses, within a health facility or hospital that may have been made via a referral from your primary care clinician (e.g. your GP). Secondary care data relates to information which have been sourced from these types of services.

Data linking

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 which covers attendances at a secondary care provider, e.g. an emergency department outpatient attendance, an emergency or planned inpatient stay.

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 as NHS Kernow does not have any access to patient identifiable data.

NHS Digital

The law provides some NHS bodies, particularly NHS Digital, ways of collecting sensitive personal data directly from care providers for secondary purposes, such as evaluating care provided at population level.

The dataset collected from secondary care providers, for example hospitals, by NHS Digital is referred to as the Secondary Uses Service (SUS). This 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: <https://digital.nhs.uk/about-nhs-digital>

Data may be de-identified¹ and linked 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.

The following are the types of organisations NHS Digital receives data from, and then forwards on to the DSCRO (our data processor) in an anonymised format or a de-identified format with NHS Number in order to link and analyse the data. Where data is used for these statistical purposes, stringent measures are taken to ensure individuals cannot be identified.

Types of organisations and types of information we receive from the Data Services for Commissioners Regional Offices (DSCRO):

- Acute trust hospitals, for example Royal Cornwall Hospital NHS Trust (RCHT) and University Hospitals Plymouth NHS Trust (UHP). They receive anonymised acute data such as emergency department attendances, waiting times, diagnosis, treatments, and follow ups, length of stay, discharge information and next steps.

¹ <https://www.digitalhealth.net/2018/07/nhs-digital-launches-deidentification-system/>

- Community trusts or community organisations, for example Cornwall Partnership NHS Foundation Trust (CPFT). They receive anonymised 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 – CPFT for Cornwall. They receive anonymised 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. They receive anonymised primary care data such as attendances, diagnosis, treatment, GP or GP practice visits, referrals, medication/prescriptions information and follow-ups.

We are required by law to report certain information to the appropriate authorities such as NHS Digital. The information may include basic details about you, such as your name and address, NHS number and date of birth but in some instances may also contain more sensitive information* about your health and also information such as outcomes of needs assessments. There may be a performance monitoring role of services, which includes responding to any concerns from patients and/or the general public on the services offered and which are dealt with through, for example, complaints department.

*Sensitive personal data is personal data consisting of information as to:

- a) The racial or ethnic origin of the individual.
- b) His/her political opinions.
- c) His/her religious or philosophical beliefs or other beliefs of a similar nature.
- d) Whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992).
- e) His/her genetic data for example those aspects relating to the inherited or acquired genetic characteristics.
- f) His/her biometric data where used for identification purposes, for example fingerprint scanning or facial recognition.
- g) His/her physical or mental health condition(s).
- h) His/her sexual life.
- i) The commission or alleged commission by him/her of any offence.
- j) Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Data processors

We may contract with other organisations to process data on our behalf. 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.

NHS Kernow uses the following data processors:

- Royal Cornwall Hospital NHS Trust (RCHT): for purposes of staff payment, pensions, recruitment, occupational health and for IT support services.
- Cornwall Partnership Foundation NHS Trust (CPFT): for records management, archiving services and the management of subject access requests.
- Data Services for Commissioners Regional Office (DSCRO): for NHS Kernow this is the South, Central and West Commissioning Support Unit – for data linkage purposes.

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 a patient needs hospital treatment while away from home on holiday. The hospital at which the patient is seen may need to invoice the patient's own CCG for the treatment they received.

Before paying, the CCG will need to be sure that they are responsible for the patient and that the amount they are being billed for is correct. This process is known as invoice validation. For invoice validation to occur, a limited amount of information about the patient needs to be shared between the organisations concerned.

The use of your information for this purpose has been allowed under s251 of the NHS Act 2006, for more information please visit: <https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/>

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 sensitive personal data to undertake risk stratification, also known as case finding.

Risk stratification is a process that uses personal data from health care services to determine which people are at high risk of experiencing certain outcomes, such as unplanned hospital admissions.

Risk stratification tools can be useful in analysing the overall health of a population (known as 'risk stratification for commissioning') and for identifying which patients should be offered targeted preventative support to reduce those risks (known as 'risk stratification for case finding'). These tools use a mix of limited historical information about patients (such as age, gender, diagnoses, and hospital attendance) as well as data collected in GP practices.

Your GP surgery uses the services of the DSCRO, NHS South, Central and West Commissioning Support Unit (<https://www.scwcsu.nhs.uk/>) to identify those most in need of preventative or improved care. This contract is arranged by NHS Kernow.

Neither NHS Kernow nor the DSCRO 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.

The DSCRO will 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 patients 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 the DSCRO for risk stratification purposes.

Your GP will provide information about any risk stratification programmes they are planning to use. The GPs can use their data to identify which of their patients would benefit from a certain preventative service. Risk stratification is a helpful tool to support GPs in identifying patients at risk.

The lawful basis to use this information for risk stratification has been allowed by s251 NHS Act 2006 and is processed by the DSCRO or other approved providers only. For further information on risk stratification, please visit: <http://www.england.nhs.uk/ourwork/tsd/ig/risk-stratification/>

Information sharing with non-NHS organisations

Information may be required to be shared for your benefit with non NHS organisations, from which you are also receiving care, such as social services, out-of-hours-service, NHS 111 or other providers from whom services are commissioned. Where information sharing with third parties is required, health information will not be disclosed without your explicit consent, unless there are exceptional circumstances, such as when the health or safety of others is at risk or where the law requires it.

We may be asked to share basic information about you, such as your name and address which does not include sensitive information but this would normally be to assist other organisations to carry out their statutory duties. In these circumstances, where it is not practical to obtain your explicit consent, we are informing you through

this notice, which is referred to as a Privacy Notice, under the Data Protection Act (2018).

Non-NHS organisations may include, but are not restricted to: education services, local authorities, the police, voluntary and private sector providers.

We will not share information about you for any reason unless:

- You have consented for us to do so.
- Where a formal court order has been served on us.
- In order to assist the police in the prevention and detection of crime.
- To protect children and vulnerable adults.
- We have special permission for health and research purposes (granted by the Health Research Authority).
- For the health and safety of others, for example to report an infectious disease such as meningitis or measles.

Patient rights

Where NHS Kernow is processing an individual's personal data they have the following rights:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relations to automated decision making and profiling.

These rights are set out in the Data Protection Act 2018, the Common Law Duty of Confidentiality and the NHS Constitution. For more information visit the Information Commissioners website: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/>

Your right to withhold consent to share your information is not absolute. In the exceptional circumstances where we are unable to do this NHS Kernow will always explain their rationale and it will be done in accordance with duties and responsibilities laid out within the Data Protection Act 2018.

When you request to withhold consent is respected and carried out, please be aware this may adversely affect the care you currently receive or may receive in the future. Always consult your GP or relevant health professional before deciding to withhold consent to sharing your information, as they will be able to advise you on the possible outcomes of this decision.

There are two types of opt out. You can apply for either opt-out at any time at your GP practice.

Type 1 opt-out

If you do not want information that identifies you to be shared outside your GP practice, for purposes other than 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 - out

NHS Digital collects information from a range of places where people receive care such as hospitals and community services.

Patients are able to opt out of their personal confidential data being shared by NHS Digital for purposes other than their own direct care. This is known as the 'type 2 opt- out'. If you do not want your personal confidential information to be shared outside of NHS Digital for purposes other than for your direct care you can register a type 2 opt-out with your GP practice.

Records for patients who have registered a type 2 opt-out will be identified using a particular code that will be applied to your medical records that will stop your records from being shared outside of your GP practice.

For further information and support relating to opt-outs, please refer to the following:

- <https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/how-we-look-after-your-health-and-care-information/your-information-choices/opting-out-of-sharing-your-confidential-patient-information>
- <https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/how-we-look-after-your-health-and-care-information/your-information-choices/how-opt-outs-work>
- Call NHS Digital on 0300 303 5678.
- For more information about care records and how to access them see NHS Choices at the following link: <https://www.nhs.uk/using-the-nhs/about-the-nhs/how-to-access-your-health-records/>
- For details about how public bodies must make information available, see the model publication scheme published by the Information Commissioner's Office, available here: <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: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>. The retention schedules start on page 53.

When destroying personal data we ensure that we, or third parties we contract to destroy data on our behalf, meet guidelines set out within principle five (storage limitation) of the Data Protection Act 2018, the European Standard EN 15713 for paper copies and CESG standards (<http://www.secure-data-destruction.co.uk/destroy-hard-drives/>) for secure destructions of electronic data.

How you can get access to your records?

Under the Data Protection Act 2018 (and for relatives of deceased patients, the Access to Health Records Act 1990), you are entitled to receive copies of all personal information held about you. Each organisation has 30 days to provide the requested information. If however, it is complex, a further 2 month extension may be required.

Any requests made will be managed by the organisation to which you apply. You do not need to give a reason. If you want to access your records you should make a written request to (or contact by phone) the NHS organisation(s) where you are being/have been, treated or have been in contact with. You should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons.

For information held by NHS Kernow please complete the subject access request form which can be found here: <https://www.kernowccg.nhs.uk/get-info/information-governance/subject-access-requests/>.

The following websites may also provide useful information:

- Information Commissioner guidance on personal information: <https://ico.org.uk/your-data-matters/>
- Legislation information relating to Access to Health Records: http://www.legislation.gov.uk/ukpga/1990/23/pdfs/ukpga_19900023_en.pdf

Facilities may be available to allow you to view parts of your health record via computer and whilst there is no charge for the first copy of your record, NHS Kernow may be entitled to charge a reasonable amount for any further copies requested.

Caldicott Guardian and Senior Information Risk Owner (SIRO)

We have assigned a Caldicott Guardian and Senior Information Risk Owner who have oversight of the handling of personal and confidential information within NHS Kernow as well as offering support to the organisations we may buy services from.

The Caldicott Guardian is a director with responsibility for protecting the confidentiality of patient information and enabling appropriate information sharing. The Senior Information Risk Owner is the director accountable for information risk. Both roles are supported by the Information Governance Sub Committee (IGSC) which meets regularly to discuss issues related to information governance. The group is formed of senior representatives from teams within NHS Kernow and is chaired by the Deputy Director of Corporate Governance. The Deputy Director of Corporate Governance also fulfils the Data Protection Officer (DPO) role for the organisation.

Our Caldicott Guardian, SIRO and DPO can be contacted at the address and telephone number below via the Corporate Governance Team.

Employee information

We collect information about individuals who work for us for the following purposes:

- The administration of prospective, current and past employees including self-employed, contract personnel, temporary staff or voluntary workers.
- The recruitment and selection process.
- Administration of non-NHS Kernow staff contracted to provide services on our behalf.
- Planning and management of our workload or business activity.
- Occupational health service.
- Administration of agents or other intermediaries.
- Pensions administration.
- Payment administration.
- Declarations of interest including gifts and hospitality received or refused.
- Appraisal, sickness, grievance, disciplinary matters, staff disputes, employment tribunals.
- Staff training and development.
- Ensuring staff are appropriately supported in their roles.
- Vetting checks.
- Assessing our performance against equality objectives as set out by the Equality Act 2010.
- Staff/workforce information is used for scenario modelling to support planning of future service provision.

Members of staff can apply for a copy of the records we hold about them by following the same processes outlined above in 'How you can get access to your records'.

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 NHS Kernow 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. More recent conflict of interest guidance was issued for clinical commissioning groups by NHS England in June 2017: <https://www.england.nhs.uk/publication/managing-conflicts-of-interest-revised-statutory-guidance-for-ccgs-2017/>.

NHS Kernow is required to publish its Registers of Interests detailing the declarations of all staff and others working with NHS Kernow. There is a process for exempting publication of individual declarations in certain exceptional and approved circumstances. Copies of the declaration of interest register, as well as the gifts and hospitality register, are held at: Sedgemoor Centre, Priory Road, St Austell PL26 5AS and can be obtained from the Corporate Governance team by phoning 01726 627800 or emailing kccg.corporategovernance@nhs.net.

Questions or concerns

If you have any questions or concerns about the information held about you or how it is used, you can get in touch by post, e-mail or via online feedback forms.

Further information can also be obtained from the Data Protection Act 2018, the General Data Protection Regulations and the Information Commissioners Office. The following links may be useful:

- <https://ico.org.uk/>
- <https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>
- <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga>
- <https://digital.nhs.uk/data-and-information/looking-after-information>

Changes to this privacy notice

We keep our privacy notice under regular review. This Privacy Notice was last updated in December 2018.

Contact the Information Governance team

Information Governance team
NHS Kernow Clinical Commissioning Group
Sedgemoor Centre
Priory Road
St Austell PL25 5AS
Telephone: 01726 627800
Email: kccg.corporategovernance@nhs.net