

Privacy Notice – Trust-Wide

This privacy notice tells you what to expect us to do with your personal data when you contact us or use our services.

Our contact details

Name: North Staffordshire Combined Healthcare NHS Trust
 Address: Lawton House, Bellringer Road, Trentham Stoke-on-Trent ST4 8HH
 General phone number: 0300 123 1535
 Website: www.combined.nhs.uk

We are the controller for your data. A controller decides on why and how data is used and shared.

Data Protection Officer contact details

Our Data Protection Officer is Sahra Smith and is responsible for monitoring our compliance with data protection requirements. You can contact her with queries or concerns relating to the use of your personal data at DPO@combined.nhs.uk.

How do we get your data and why do we have it?

The healthcare professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment. NHS health records may be electronic, paper-based or a mixture of both. We use a combination of working practices and technology to ensure that your data is kept confidential and secure.

The personal data we collect is provided directly from you for one of the following reasons:

- You have provided data to seek care – this is used directly for your care and also to manage the services we provide, to clinically audit our services, investigate complaints or to be used as evidence as part of an investigation into care
- To contact you – when you attend one of our sites, you may be asked to confirm your details such as telephone number, email address and mobile phone number (be advised that we will use your mobile phone number to send you text reminders regarding your upcoming appointments – if you want to opt out of this text message reminder service, need to change your details or have any concerns about an appointment reminder text message you have received, please contact your clinical team whose details will be on your appointment letter).
- You have applied for a job with us or work with us
- You have signed up to a newsletter, survey or other communication (you have the right to opt out of taking part/subscribing)
- You have made a complaint

We also receive personal data about you indirectly from other health and care organisations involved in your care so that we can provide you with care and from family members or carers to support you.

Categories and Sources of Personal Data

This list is not exhaustive:



Chairman: David Rogers
 Chief Executive: Dr Buki Adeyemo
www.combined.nhs.uk

Follow us on Twitter: @CombinedNHS
 Follow us on Facebook: www.facebook.com/NorthStaffsCombined



We are a diverse and inclusive Trust and there is no place in our organisation for discrimination, harassment or personal abuse

Trust Business Activities	Mental and physical healthcare Access and assessment teams Primary care teams Learning disability services Child and adult protection Population Health Management	Risk Stratification Service Development and Planning Human resources (including DBS checks) Payroll and finance Procurement Estates and facilities (maintenance) Occupational health Volunteers Goods and services
Personal data we may process	Personal details Family details Education, training Employment details Financial details	Lifestyle and social circumstances Visual images, personal appearance and behaviour Details held on patients' records Responses to surveys
Sensitive personal data we may process	Racial and ethnic origin Offences and alleged offences Criminal proceedings, outcomes and sentences Genetics	Physical or mental health details Religious or similar beliefs Sexual life Biometrics (where use for ID Purposes)
We process data about	Patients Suppliers Employees Volunteers	Complaints Survey respondents Professional experts and consultants Individuals captured by CCTV images
Sources of data we process	Our Health Records Other health and social care providers Local and national health and social care organisations	Local and regional shared care records Contractors and Suppliers Professional bodies Data subjects

Who do we share data with?

We will share data with the following organisations:

Other NHS Trusts and hospitals that are involved in your care
Ambulance Trusts
GP Practices & Primary Care Networks (PCNs)
NHS Bodies
Commissioning Support Units
Independent Contractors such as dentists, opticians, pharmacists
Other 'data processors' which you will be informed of

Private Sector Providers
Voluntary Sector Providers
Social Care Services
Local Authorities
Education Services
Fire and Rescue Services
Police & Judicial Services

In some circumstances we are legally obliged to share data, without your consent. This includes:

- When required by NHS England to develop national IT and data services
- When reporting births, deaths and some infectious diseases
- When a court orders us to do so
- Where a public inquiry requires the data

We will also share data if the public good outweighs your right to confidentiality. This could include:

- Where a serious crime has been committed
- Where there are serious risks to the public or staff
- To protect children or vulnerable adults

We may also process your data in order to de-identify it, so that it can be used for purposes beyond your direct care whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

When we need to share your personal data with third parties that are not health and social care providers, such as relatives, the common law duty of confidentiality must still be met through consent. Where a child is under the age of 13,

then consent (under the common law duty of confidentiality) of those with parental responsibility will be sought. These types of requests may include requests from organisations or solicitors who have been given authority in writing to act on behalf of the individual concerned.

Integrated Care Record – One Health and Care

Data regarding your health and care is recorded across NHS organisations and local authorities. One Health and Care pulls the key data from these different health and social care systems and displays it in one combined record. This enables registered health and social care professionals involved in your care to find all the key, most up-to-date data in one place which helps to provide better, safer care.

Click [here](#) for more information.

What is our lawful basis for using data?

Personal data

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal data is:

- (c) We have a legal obligation – the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See [this list](#) for the most likely laws that apply when using and sharing data in health and care.
- (e) We need it to perform a public task – a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities by law. See [this list](#) for the most likely laws that apply when using and sharing data in health and care.

More sensitive data

Under UK GDPR, the lawful basis we rely on for using data that is more sensitive (special category) is:

- (b) We need it for employment, social security and social protection reasons (if authorised by law). See [this list](#) for the most likely laws that apply when using and sharing data in health and care.
- (f) We need it for a legal claim or the courts require it.
- (h) To provide and manage health or social care (with a basis in law). See [this list](#) for the most likely laws that apply when using and sharing data in health and care.
- (i) To manage public health (with a basis in law). See [this list](#) for the most likely laws that apply when using and sharing data in health and care.
- (j) For archiving, research and statistics (with a basis in law). See [this list](#) for the most likely laws that apply when using and sharing data in health and care.

What are your data protection rights?

Under data protection law, you have rights including:

Your right to be informed – as a controller, we are required to inform individuals when their personal data is collected and about the intended purposes behind the processing of that data. This privacy notice ensures that as an organisation, we satisfy this right.

Your right of access – you have the right to request access to and/or copies of your personal data we hold about you, free of charge (subject to exemptions) – this is known as a [subject access request](#).

We will aim to provide your data within **one calendar month** as required by law and will notify you if this is not possible for whatever reason. Requests can be made verbally or in writing, but we do ask that you provide us with adequate data to process your request, such as providing full name, address, date of birth, NHS number and details of your request and, where necessary, any documents to verify your identity.

On processing a request there may be occasions when data may be withheld if we as an organisation believe that releasing the data to you could cause serious harm or distress.

Data may also be withheld if another person (i.e., a third party) is identified in the record, and they do not want their data disclosed to you. However, if the other person mentioned in your records was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that data.

How to access your personal data

To request access to the personal data we hold about you please click on the following link which takes you to our secure Subject Access Request portal and follow the 'Get Started Online' instructions on the opening page:

[Home Page - Portal \(ams-sar.com\)](https://ams-sar.com)

For further assistance or enquires please contact:

Tel: 0300 123 1535 or **Email:** IG@combined.nhs.uk

Your right to rectification – you have the right to have inaccurate (incorrect or misleading) personal data corrected by us without undue or excessive delay. Taking account of the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If however, such requests are linked to legally significant matters, such as confirming legal identity, we may require proof of any alleged inaccuracy before we are able to rectify the data held.

Every time you attend a site operated by us, please check that the correct contact details are recorded for you and be prepared to have data checked at every appointment/telephone call.

Your right to erasure – you have the right to have your personal data erased or deleted. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose which it was originally collected or processed for, or if you wish to withdraw your consent after you have previously given your consent.

Your right to restrict processing – you have the right to ask us to restrict the processing of your personal data when one of the following applies:

- You contest the accuracy of your personal data and we are investigating
- We no longer need your personal data, but you need it to be kept for legal claims
- The processing is unlawful, but you oppose erasure of your personal data
- You have objected to us processing your personal data and we are considering whether our legitimate grounds override yours

Your right to object to processing – You have the right to object to us processing your personal data on grounds relating to your particular situation and to data processed for direct marketing purposes where the processing is based on:

- legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

This right does not apply where we can demonstrate compelling legitimate grounds for the processing of your personal data.

If we did not process any personal data about you and your health care needs it would be very difficult for us to care for and treat you.

Your right to data portability -You have the right to ask that we transfer personal data you gave us to another organisation, or to you, in a structured, commonly used and machine-readable format, if technically feasible to do so (in certain circumstances).

Your rights in relation to automated decision making and profiling - Automated individual decision-making is a decision made by automated means (i.e., a computer system) without any human intervention. If any of the processes we use rely on automated decision making, you do have the right to ask for a human to review any computer-generated decision at any point.

We do not conduct any automated decision making but may look to identify people who may benefit from our services (profiling). All actual decision making carried out by appropriate staff based on the data available to them.

National Opt-Out

You have a choice about whether you want your personal data used for purposes beyond your individual care, such as identifying and developing new treatments (research), preventing illnesses and diseases, monitoring safety and planning services. All these uses help to provide better health and care for you, your family and future generations.

If you are happy with this use of your personal data, you do not need to do anything. If you choose to opt-out, your confidential patient data will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit [Your NHS Data Matters](#) or you can call the NHS Digital Contact Centre on 0300 303 5678 (Monday to Friday 9am to 5pm excluding bank holidays).

There are some instances when your choice may not apply. If the data is vital to improving patient care and public health, then the Confidentiality Advisory Group of the Health Research Authority (an independent body who provide expert advice on the use of confidential patient data) can recommend an exemption in the public interest. This means that data about patients and care received can be collected even where people have chosen not to have their health data shared for reasons other than individual treatment and care.

The National Confidential Inquiry into Suicide and Safety in Mental Health (NCISH) has been recommended for an exemption from applying the NDO to the data collected. To improve safety for all mental health patients, deaths by suicide of all people under the recent care of specialist mental health services must be examined. Improvements can then be made to the quality and care offered by services. This is in the interest of patients and public alike.

You can also find out more about how patient data is used at:

[Health Records Authority](#) – patient data and health and care research

[Understanding Patient Data](#) – covers how and why patient data is used, the safeguards and how decisions are made

Please note, you can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

Storage of personal data

All the personal data we hold is held electronically on clinical systems implemented across our sites.

Cloud Storage

We use a cloud storage solution hosted by Amazon Web Services (AWS). All data that is backed up to the cloud storage solution remains in the UK and is fully encrypted both in transit and at rest. Using a cloud storage solution does not change the control of access to your personal data and the hosted service provider does not have any access to the decryption keys. AWS is one of the world's largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the very highest levels of security and support.

Scanning of Patient Records

We have implemented an electronic document management system (EDMS) to scan paper records into our main clinical system as we strive to be a paperless organisation reliant on advanced digital solutions. Having comprehensive records all in one place enables us to provide the most appropriate care for you and have all of your documents easily accessible. The EDMS has undergone rigorous checks to ensure the data is scanned safely and securely with the key assurances provided to both us and you.

Retention of Personal Data

We adhere to the NHS Records Management Code of Practice for Health and Social Care and national archives requirements regarding the retention of your personal data. More information on the relevant retention periods can be found in the [NHS Records Management Code of Practice 2021](#).

Disposal of Data when no longer required

If, following the end of the retention period, any documents need to be securely disposed of, we will ensure that any data held in manual form is destroyed using a cross-cut shredder or a reputable confidential waste company that complies with European Standard EN15713 and obtain certificates of destruction.

Electronic storage media used to store, or process data are destroyed or overwritten to national standards.

Transfers of your data to third countries or international organisations

If we need to transfer your personal data overseas, it will only be shared within the European Economic Area (EEA) unless additional safeguards have been implemented to protect your data. At all times, current data protection legislation will be complied with.

We will inform you if your personal data needs to be transferred.

Closed Circuit Television (CCTV)

We use CCTV systems for crime prevention in line with the Information Commissioner's Office guidance and the Surveillance Camera Code of Practice. You have the right to request your data captured on CCTV.

Third-party processors

We will use carefully selected third-party service providers, as necessary. When we use a third-party service provider to process data on our behalf, we will always have an appropriate agreement in place to ensure that they keep the data secure, do not use or share it other than in accordance with our instructions and that they are operating appropriately.

These third-party service providers include companies that provide IT services and support (including our core clinical systems), systems that manage patient facing services, data hosting service providers, systems that facilitate appointment bookings or electronic prescription services, document management services, delivery services, payment providers and confidential waste companies. This list is not exhaustive and further details of our third-party processors can be supplied on request.

Complaints and your right to complain to the regulator

You can complain directly to us if you are concerned about how we process your personal data. In the first instance, a complaint should be made to our Data Protection Officer.

You can also raise a complaint with the Patient Experience Team, who are available Monday-Friday 9am-5pm.

You also have the right to lodge a complaint with the UK's independent authority on data protection issues, the Information Commissioner's Office.

Data Protection Officer

North Staffordshire Combined Healthcare NHS Trust

Lawton House

Bellringer Road

Trentham

Stoke-on-Trent ST4 8HH

Email: DPO@combined.nhs.uk

Patient Experience Team

Email: patientexperienceteam@combined.nhs.uk

Telephone: 01782 275301

Freephone: 0800 389 9676

Text: 07718 971 123 (please note that this text service is available Monday to Friday 9am-5pm only and is charged at your provider's rate)

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Telephone: 01625 545745 www.ico.gov.uk