Conexus Healthcare CIC,
Sandal Castle Medical Centre, Asdale Rd, Wakefield, West Yorkshire, WF2 7JE

Data Protection Privacy Notice for Patients

Introduction

This privacy notice lets you know what happens to any personal data that you give to us, or any information that we may collect from you or about you from other organisations.

This privacy notice applies to personal information processed by, or on behalf of, Conexus Healthcare.

We will never pass on your personal information to anyone else who does not need it, or has no right to it, unless you give us consent to do so.

This notice explains:

- Who we are and how we use your information
- Information about our Data Protection Officer
- What kinds of personal information about you we hold and use (process)
- The legal grounds for our processing of your personal information (including when we share it with others)
- What to do if your personal information changes
- How long your personal information is retained / stored by us
- What your rights are under Data Protection laws

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) replaced the previous Data Protection Act (1998) and govern how we use your personal data. They have since been amended, including by the Data (Use and Access) Act 2025.

For the purpose of applicable data protection legislation (including, but not limited to, the UK General Data Protection Regulation (UK GDPR), and the Data Protection Act (DPA) 2018), the organisation responsible for your personal data is Conexus Healthcare.

This Notice describes how we collect, use, and process your personal data, and how in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

Why we need your information

The healthcare professionals who provide you with care need to 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 information is kept confidential and secure.

Records about you may include the following information:

- Details about you such as your address, your carer or legal representative and emergency contact details.
- Any contact the surgery has had with you such as appointments, clinic visits, emergency

Registered name: Conexus Healthcare (10772469)
Sandal Castle Medical Centre, Asdale Road, Wakefield, England, WF2 7JE
V10- June 2026

appointments.
- Notes and reports about your health.
- Details about your treatment and care.
- Results of investigations such as laboratory tests, x-rays, etc.
- Relevant information from other health professionals, relatives or those who care for you.
- Contact details (including email address, mobile telephone number and home telephone number).

To ensure you receive the best possible care, your records are used to facilitate the care you receive, and this may include contacting you. Information held about you may be used to help protect the health of the public and to help us manage the NHS and the services we provide. Limited information may be used by the organisation for clinical audit to monitor the quality of the service we provided.

Our lawful basis for using your information

Personal information

Under Article 6 (1) of the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for using personal information are:

(a) We have your consent – this is gained specifically for some website cookies, procedures, marketing or research for example.

(b) We are performing a public task – under Article 6 (1)(e), most of our processing is necessary for the performance of tasks carried out in the public interest, namely the delivery of healthcare services we are commissioned to provide under our contracts with NHS West Yorkshire Integrated Care Board and Wakefield Council.

(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.

(d) If it is in your vital interest – if you require healthcare but are not in a position to consent, such as in the case of a medical emergency.

More sensitive data

Some kinds of information, such as sensitive healthcare records, require additional conditions to be met. Our reasons, under Article 9 (2) of the UK GDPR are as follows. That the processing of data is necessary for:

(h and c) the reasons of preventative or occupational medicine, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Occasionally when it is necessary to protect the vital interests of a person who is physically or legally incapable of giving consent.

(a) cases where explicit consent has been given to process the information for a purpose or purposes.

(f) the establishment exercise or defending of legal claims or whenever courts are acting in their judicial capacity.

(g and i) interests of public interest, with a basis in law, or public health.

(j) archiving, research, and statistics.

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

We use your personal and healthcare information in the following ways:

- when we need to speak to or contact other doctors, consultants, nurses or any other medical/healthcare professional or organisation during the course of your diagnosis or treatment or ongoing healthcare;

- when we are required by law to hand over your information to any other organisation, such as the police, by court order, solicitors, or immigration enforcement.

Risk Stratification

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from GP Practices. The identifying parts of your data are removed, analysis of your data is undertaken, and a risk score is then determined. This is then provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt-out of your data being used in this way in most circumstances. Please contact your GP practice for further information about opting out.

Anonymised Information

Sometimes we may provide information about you in an anonymised form. Such information is used to analyse population-level heath issues and helps the NHS to plan better services. If we share information for these purposes, then none of the information will identify you as an individual and cannot be traced back to you.

Care Connect Service

The Care Connect service allows authorised clinical staff at NHS 111 to seamlessly access our clinical system and book directly on behalf of a patient. This means that should you call NHS 111 and the clinician believes you need an appointment, the clinician will access available appointment slots only (through GP Connect) and book you in. This will save you time as you will not need to contact the GPCW direct for an appointment.

The organisation will not be sharing any of your data and will only allow NHS 111 to see available appointment slots. They will not even have access to your record. However, NHS 111 will share any relevant data with us, but you will be made aware of this. This will help your GP in knowing what treatment / service / help you may require.

Please note if you no longer require the appointment or need to change the date and time for any reason you will need to speak to one of our reception staff and not NHS 111.

Patient Communication

Because we are obliged to protect any confidential information that we hold about you and we take this very seriously, it is imperative that you let us know immediately if you change any of your contact details.

We may contact you using SMS texting to your mobile phone in the event that we need to notify you about appointments and other services that we provide to you involving your direct care. Therefore, you must ensure that we have your up-to-date details. This is to ensure we are sure we are actually contacting you and not another person. As this is operated on an 'opt-out' basis we will assume that you give us permission to contact you via SMS, if you have provided us with your mobile telephone number. Please let us know if you wish to opt-out of this SMS service. We may also contact you using the email address you have provided to us. Please ensure that we have your up-to-date details.

There may be occasions where authorised research facilities would like you to take part in research. Your contact details may be used to invite you to receive further information about such research opportunities.

Safeguarding

The organisation is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied with the wellbeing of all, at the heart of what we do.

Our legal basis for processing in these cases for the UK General Data Protection Regulation (UK GDPR) purposes is: -

> *Article 6(1)(e) '…exercise of official authority…'.*

For the processing of special categories data, the basis is: -

> *Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'*

Categories of personal data

The data collected by staff in the event of a safeguarding situation will be as much personal information as is possible that it is necessary to obtain in order to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Sources of the data

The organisation will either receive or collect information when someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

Recipients of personal data

The information is used when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e., their GP or Mental Health team).

Research

Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here: -

https://cprd.com/transparency-information

The legal bases for processing this information

CPRD do not hold or process personal data on patients; however, NHS England (which has incorporated the former NHS Digital, formerly the Health and Social Care Information Centre) may process 'personal data' for us as an accredited 'safe haven' or 'trusted third-party' within the NHS when linking GP data with data from other sources. The legal bases for processing this data are:

- Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) - public interest in the area of public health
- Medical research and statistics: Article 6(e) and Article 9(2)(j) - public interest and scientific research purposes

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

Third party processors

In order to deliver the best possible service, we will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, we will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties include:

- Companies that provide IT services and support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services, etc.
- Delivery services (for example, if we were to arrange for delivery of any medicines to you).
- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third-party processors can be supplied on request to the Data Protection Officer as below.

How we maintain the confidentiality of your records

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR)
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation or in an NHS commissioned organisation has a legal obligation to keep information about you confidential.

Common law duty of confidentiality

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- you have provided us with your consent (we have taken it as implied to provide you with care, or you have given it explicitly for other uses)
- we have a legal requirement to collect, share and use the data
  for specific individual cases, we have assessed that the public interest to share the data overrides the public interest served by protecting the duty of confidentiality (for example sharing information with the police to support the detection or prevention of serious crime). This will always be considered on a case-by-case basis, with careful assessment of whether it is appropriate to share the particular information, balanced against the public interest in maintaining a confidential health service.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Our policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the UK General Data Protection Regulation (UK GDPR) and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged are asked to sign a confidentiality agreement. If required, we will sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Conexus Healthcare an appropriate contract (art 24-28) will be established for the processing of your information.

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the Data Protection Officer in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – your surgery will always gain your

consent before releasing the information for this purpose in an identifiable format. In some circumstances you can opt-out of your surgery sharing any of your information for research purposes.

Consenting to additional sharing of information

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details and email address to inform you of other services that may benefit you. We will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt into such programmes if you are happy to do so.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt-out prior to any data processing taking place.
This information is not shared with third parties or used for any marketing, and you can unsubscribe at any time via phone, email or by informing the DPO as below.

Where do we store and share your information electronically?
All the personal data we process is processed by our staff in the UK. However, for the purposes of IT hosting and maintenance this information may be located on servers within the European Union. Where this happens, the transfer is protected by the UK's adequacy regulations for the EU/EEA or other transfer safeguards approved under UK data protection law.

No third parties have access to your personal data unless the law allows them to do so, and appropriate safeguards have been put in place such as a Data Processor as above. We have a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data. We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations;

- NHS Trusts / Foundation Trusts
- General Practices
- Primary Care Network
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Integrated Care Boards (ICBs)
- Social Care Services
- NHS England (NHSE), which now incorporates the former NHS Digital
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Private Sector Providers
- Other 'data processors' which you will be informed of

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

Computer System

We operate a Clinical Computer System on which NHS Staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history, including allergies and medication.

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisations (above). Wherever possible, their staff will ask your consent before your information is viewed.

National Data Opt Out

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt-out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt-out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number, if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

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

https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and

https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)

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.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems. You can opt-out of this sharing of your records with our partners at any time, if this sharing is based on your consent.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for Conexus Healthcare an appropriate contract (art 24-28) will be established for the processing of your information.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- where there is a serious risk of harm or abuse to you or other people
- Safeguarding matters and investigations
- where a serious crime, such as assault, is being investigated or where it could be prevented
- notification of new births
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS)
- where a formal court order has been issued
- where there is a legal requirement, for example if you had committed a Road Traffic Offence.

How long will we store your information

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

Your rights relating to the personal data that you have given to us

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data and you do not agree, you have the right to object. We will respond to your request within one month (although we may be allowed to extend this period in certain cases). This is NOT an absolute right as sometimes we will need to process your data even if you object.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project, or you have consented to us sending you information about us or matters you may be interested in), you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within one month (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will need to keep a note of your name/other basic details on our register of individuals who would prefer not to be contacted. This enables us to avoid contacting you in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. Where necessary, we will help with this with a GP-to-GP data transfer and transfer of your hard copy notes where we hold them.

Accessing the information we hold about you

Subject Access Requests (SAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the organisation holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

- Your request should be made to the IG Lead, Conexus Healthcare CIC
- **Head Office: Conexus Healthcare CIC**
  C/O Sandal Castle Medical Centre
  Asdale Road
  Wakefield
  WF2 7JE
- Or by email: **wyicb-wak.conexussar@nhs.net**
- (For information from a hospital or other Trust/ NHS organisation you should write direct to them).
- There is no charge to have a copy of the information held about you
- We are required to provide you with information within one month
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located.

What to do if your personal information changes

You should tell your surgery so that they can update their records. Please contact them as soon as any of your details change, this is especially important for changes of address or contact details (such

as your mobile phone number). From time to time your surgery will ask you to confirm that the information we currently hold is accurate and up to date.

CCTV

We employ surveillance cameras (CCTV) on and around our sites in order to:

- protect staff, patients, visitors and organisation property
- apprehend and prosecute offenders, and provide evidence to take criminal or civil court action
- provide a deterrent effect and reduce unlawful activity
- help provide a safer environment for our staff
- assist in traffic management and car parking schemes
- monitor operational and safety related incidents
- help to provide improved services, for example by enabling staff to see patients and visitors requiring assistance
- assist with the verification of claims

You have a right to make a Subject Access Request of surveillance information recorded of yourself and ask for a copy of it. Requests should be directed to the address below and you will need to provide further details as contained in the section 'How you can access your records'. The details you provide must contain sufficient information to identify you and assist us in finding the images on our systems. If the site is owned by another organisation, then you will need to make the request to them, for example if you are on a hospital site.

We reserve the right to withhold information where permissible by the UK GDPR and we will only retain surveillance data for a reasonable period or as long as is required by law. In certain circumstances (high profile investigations, serious or criminal incidents) we may need to disclose CCTV data for legal reasons. When this is done there is a requirement for the organisation that has received the images to adhere to the UK GDPR.

Objections / Complaints

Should you have any concerns about how your information is managed, please contact us or the Data Protection Officer as below.

By email:
wyicb-wak.conexuscontact@nhs.net
By post:
IG Lead
Head Office: Conexus Healthcare CIC
C/O Sandal Castle Medical Centre
Asdale Road
Wakefield
WF2 7JE

The Data Protection Officer is Helen Holt from The Health Informatics Service. Any queries regarding Data Protection issues should be addressed to her at:

Email: Helen.Holt@this.nhs.uk
Post: The Health Informatics Service
Unit 13 Ainley Industrial Estate
Ainley Bottom
Elland

HX5 9JP

If you are unhappy with the way we have handled your personal data, you have the right to make a complaint to us. We take all data protection complaints seriously and have a process in place to deal with them. You can make a complaint by emailing or writing to the IG Lead or the Data Protection Officer using the contact details above, or by speaking to a member of staff. To help us deal with your complaint efficiently, please include your name and contact details, a description of your concern, and any relevant dates or reference numbers.

When we receive your complaint, we will acknowledge it within 30 days. We will then investigate your concerns, take appropriate steps to address them, and inform you of the outcome of your complaint without undue delay. Raising a complaint will never affect the care you receive from us.

If you are still unhappy following our response, you have a right to lodge a complaint with a supervisory authority: The UK's supervisory Authority can be contacted as follows:

Information Commissioner:
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

https://ico.org.uk/

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact the Data Protection Officer.

Changes:

It is important to point out that we may amend this Privacy Notice from time to time. If you are dissatisfied with any aspect of our Privacy Notice, please contact the Data Protection Officer.

Updated June 2026