

Data Protection Privacy Notice for Patients

Introduction

For the purpose of applicable data protection legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, the GP practice responsible for your personal data is **Charnwood Surgery**.

We, Charnwood Surgery, are the 'Controller' of the personal data you provide to us. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

This Privacy Notice applies to personal information processed by or on behalf of the Practice. It applies to the personal data of our patients and to the data you have given us about your carers/family members. This notice includes specific information for children and young people.

Contents

- Why do we need your data?
- What data do we collect about you?
- What is the legal basis for using your data?
- How do we store your data?
- Our systems and data processors
- Privacy notice for children and young people
- How do we maintain the confidentiality of your data?
- How long do we keep your data?
- What are your data protection rights?
- Who do we share your data with?
- Are there other projects where your data may be shared?
- When is your consent not required?
- How can you access or change your data?
- What should you do if your personal information changes?
- Changes to our privacy policy
- Our Data Protection Officer
- How to contact the appropriate authorities

Why do we need your data?

As your General Practice, we need to know your personal, sensitive and confidential data in order to provide you with appropriate healthcare services. Your records are used to facilitate the care you receive, and to ensure you receive the best possible healthcare.

Information may be used within the GP practice for clinical audit, to monitor the quality of the service provided.

What data do we collect about you?

Personal data

We collect basic personal data about you which does not include any special types of information or location-based information. This includes your name, postal address and contact details such as email address and telephone number.

By providing the Practice with your contact details, healthcare communications via these channels (letter, voicemail, SMS, email) are processed under **public task** (Article 6(1)(e) UK GDPR) for direct care. You can opt out at any time by contacting us.

Special Category personal data

We also collect confidential data linked to your healthcare which is known as "special category personal data", in the form of health information, religious belief (if required in a healthcare context) ethnicity and gender. This is obtained during the services we provide to you and through other health providers or third parties who have provided you with treatment or care, e.g. NHS Trusts, other GP surgeries, Walk-in clinics etc.

Records which the Practice holds about you may include the following information:

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

NHS records may be electronic, on paper, or a mixture of both.

Use of CCTV

Closed circuit television is utilised to protect the safety of our patients, staff and members of the public. To maintain privacy and dignity, CCTV is not in place where examinations or procedures are being undertaken. The Practice remains the data controller of this data and any disclosures or requests should be made to the Practice Manager.

What is the legal basis for using your data?

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

- Data Protection Act 2018
- 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

Under the UK GDPR, we primarily rely on:

Article 6(1)(e) - "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

Article 9(2)(h) - "processing is necessary for the purposes of preventive or occupational medicine... medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems"

We also rely on Article 6(1)(b) for contractual processing (patient registration) and Article 9(2)(i) for public health tasks (vaccination monitoring, population health).

These articles apply to the processing of information and the sharing of it with others for specific purposes.

How do we store your data?

We have a Data Protection regime in place to oversee the effective and secure processing of your personal and special category (sensitive, confidential) data. 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.

In certain circumstances you may have the right to withdraw your consent to the processing of data. These circumstances will be explained in subsequent sections of this document.

In some circumstances we may need to store your data after your consent has been withdrawn, in order to comply with a legislative requirement.

Data processors are UK/EU-based with adequacy decisions or Standard Contractual Clauses per UK GDPR Art 46.

Our systems and data processors

To deliver safe and effective healthcare, we use a number of systems and work with trusted data processors. These organisations process your data under our instruction and are bound by strict data protection agreements.

SystemOne (TPP)

SystemOne is our primary clinical system, provided by TPP (The Phoenix Partnership). It stores your complete electronic medical record and enables:

- Recording of all clinical consultations, treatments and care
- Secure access for authorised healthcare professionals within the practice
- GP Connect sharing for direct care purposes with other NHS organisations
- Comprehensive audit trail of all record access
- Online services access via NHS App

SystemOne operates under robust security controls with role-based access permissions. All staff access to records is logged and monitored.

GP Connect

GP Connect enables your GP record to be securely shared with other NHS organisations (such as hospitals, 111 services, and other GP practices) when you receive care outside of this practice. This allows healthcare professionals involved in your direct care to access relevant parts of your medical record in real-time, improving safety and reducing the need for you to repeat information.

GP Connect operates within the SystemOne system using secure NHS infrastructure. Only healthcare professionals directly involved in your care can access your information, and all access is logged and auditable.

AccuRx

AccuRx enables secure digital communication between the practice and patients via SMS, email, and video consultations. It is used for:

- Appointment confirmations and reminders
- Two-way SMS messaging about clinical matters
- Video consultations
- Questionnaire distribution
- Results and prescription notifications

All patient data is encrypted end-to-end, processed under strict DPA, and never stored by AccuRx beyond message delivery. You control your contact preferences and can opt out of SMS/email communications at any time. AccuRx integrates securely with SystmOne.

Ardens Manager

Ardens Manager provides clinical templates, coding support and population health analytics within our SystmOne system. It processes pseudonymised patient data (no names or NHS numbers) to help us:

- Deliver standardised, high-quality care
- Monitor disease registers and QOF performance
- Identify patients needing proactive support
- Improve clinical outcomes through data insights

Ardens acts as a data processor under our strict instruction with UK-based secure servers. All access is role-controlled and fully auditable. Data remains within our secure SystmOne environment.

Choose and Book / e-Referral Service (NHS e-RS)

When we refer you to a hospital or specialist service, we use the NHS e-Referral Service (formerly Choose and Book). This system allows us to book appointments electronically and enables you to choose your hospital or clinic. Your referral information is shared securely with the hospital or service you select. You can also manage your appointments online via the NHS App or NHS e-Referral website.

Child Health Information Service (CHIS)

We share information about children registered with the practice with the Child Health Information Service (CHIS) managed by the local NHS provider. CHIS maintains records of childhood immunisations, developmental checks, and screening programmes. This sharing ensures children receive appropriate health surveillance and enables the NHS to monitor vaccination coverage and public health outcomes. This is a legal requirement under public health legislation.

OPCOne

OPCOne is a secure platform that enables approved researchers and public health professionals to analyse pseudonymised GP data for research, service evaluation, and health surveillance purposes. Similar to OpenSAFELY, your data (with direct identifiers such as name and NHS number removed) remains within the secure SystmOne environment and cannot be downloaded by researchers. Only aggregate statistical results are produced. OPCOne is used by NHS England, academic institutions, and approved research organisations under strict governance and data protection agreements. The National Data Opt-Out does not apply as data is pseudonymised, but you can discuss concerns with the Practice.

Primary Care Network Data Pack

As part of Soar Valley Primary Care Network, we share pseudonymised patient data through the PCN Data Pack for quality improvement and population health management purposes. This data helps the network monitor performance indicators, identify health trends, and plan services to improve care for our local population. Individual patients cannot be identified in the aggregated reports. This sharing is conducted under Article 6(1)(e) and Article 9(2)(h) of GDPR as a public health task.

iGPR

iGPR is used to process Subject Access Requests (SARs) efficiently and securely. It enables:

- Secure extraction of your medical record
- Redaction of third-party information where required
- Preparation of records in compliance with GDPR Article 15

iGPR acts as a data processor under our instruction and all data handling complies with NHS Digital standards.

Healthtech-1

Healthtech-1 processes new patient registrations automatically, enabling:

- Efficient processing of registration forms
- Validation of patient details
- Integration with SystemOne clinical system

All registration data is handled securely and transferred directly to our clinical system.

Appliance Prescribing Service

To support safe and effective management of urology and trans-anal irrigation (TAI) appliances, prescribing for eligible adult patients may be managed by a commissioned specialist provider on behalf of Leicester, Leicestershire and Rutland Integrated Care Board (ICB).

The service oversees prescribing and ongoing prescription management for urology and TAI appliances. This is to:

- Provide appropriate clinical oversight by specialist nurses with prescribing authority
- Review prescription quantities to promote safe use and reduce waste
- Arrange prompt referral back to specialist teams if complications or concerns arise
- Improve patient experience through telephone, digital and email access for advice and ordering

Where clinically appropriate, your GP practice may transfer responsibility for prescribing these appliances to the specialist service. Your clinical care remains under the NHS, and you retain the same data protection and confidentiality rights as set out in this privacy notice.

Heidi Health

Heidi Health is an AI-powered clinical scribe used during some consultations to generate accurate consultation summaries. Heidi Health uses automated processing to create notes (no automated decisions affecting you). The system:

- Transcribes consultations in real-time with your knowledge
- Generates structured clinical notes
- Operates on UK-based secure servers
- Processes data under strict data processing agreements
- Does not retain audio recordings after transcription

Your rights regarding Heidi Health:

- You may request that Heidi Health is not used during your consultation
- The clinician will inform you when Heidi Health is active
- You can opt out at any time without affecting your care
- All generated notes are reviewed and approved by your clinician before being saved to your record

If you have concerns about the use of Heidi Health, please inform reception or your clinician before your appointment.

Data Processor Safeguards

All of our data processors are required to:

- Process data only under our written instructions
- Maintain appropriate technical and organisational security measures
- Ensure staff confidentiality obligations
- Assist with data subject rights requests
- Delete or return data when services end
- Undergo regular security audits

Privacy notice for children and young people

This section explains how we use and protect information about children and young people in simple terms. It applies to everyone under 18 who is registered at the practice.

What information do we have about you?

We keep a health record for every child and young person registered with us. This can be on computer, on paper, or both. It includes:

- Your name, date of birth, address and contact details
- Information about your parents or carers (for example, who looks after you and who we should contact in an emergency)
- Information about your appointments and visits
- Notes about your health and any treatment you receive
- Test results (like blood tests or x-rays)
- Letters and reports from hospitals, school nurses or other health professionals
- Your vaccinations and medicines

We only collect information that we need to look after your health.

Why do we need your information?

We use this information so we can:

- Help you stay healthy and feel better when you are unwell
- Keep track of your vaccinations and health checks
- Share important information with doctors, nurses or other people who look after you
- Check that the care you receive is safe and of good quality
- Help keep you and other people safe if we are worried about you

We must follow the law when we use your information and only use it when we have a good, lawful reason to do so.

Our computer systems (explained simply)

We use secure NHS computer systems to look after your information. These include:

SystemOne – This is like a very secure computer filing cabinet that keeps your health record safe. Only doctors, nurses and other practice staff who are looking after you, or need the information to help run the service, can see it.

Messaging systems (such as AccuRx) – These are secure systems we use to send text messages or emails about appointments, test results or questionnaires. They only use the contact details we have for you and your parent or carer.

Registration systems (such as Healthtech-1) – These help us safely and quickly register you as a patient when you first join the practice.

Clinical tools and planning systems (such as Ardens Manager, OPCOne, OpenSAFELY and Primary Care Network data packs) – These systems usually use coded or *pseudonymised* information (this means your name and NHS number are removed and replaced with a code) to help us and the NHS plan services, check how we are doing, and improve care for everyone. Reports from these systems do not name you.

Heidi Health – Sometimes your doctor might use a special computer helper called Heidi Health during your appointment. It listens to what you and the doctor say and helps write notes. Your doctor will tell you if they are using it, and you can ask them not to if you prefer.

All of these systems must follow strict NHS data protection and security rules.

Child Health Information Service (CHIS)

We share information about children with the Child Health Information Service (CHIS). CHIS keeps records of:

- Your vaccinations
- Your health checks and screening programmes

This helps make sure you are invited for the right vaccines and checks at the right time and helps the NHS keep track of how well vaccination and screening programmes are working. CHIS also has to follow strict rules to keep your information safe.

Who can see your information?

People who may see your information include:

- Doctors, nurses and other staff at the practice
- Other NHS services involved in your care, such as hospitals, walk-in centres, out-of-hours doctors, 111 and ambulance services
- School nurses or other health professionals supporting you at school (only when needed for your health)
- Local Child Health Information Services (CHIS) for vaccinations and checks
- People and teams whose job is to help keep you safe, such as social care, safeguarding teams or the police, if we are worried about your safety or someone else's

They can only see the information they need to do their job and must keep it private.

Your parents or carers:

- Usually, your parents or carers can see your health information and talk to us about your care.
- As you get older and are able to understand your own health and decisions (usually from around age 13, but it depends on you), you may be able to have more privacy and make some decisions for yourself.
- You can talk to your doctor or nurse about what this means for you, including when information might be kept private from your parents or carers.

Keeping you safe

Sometimes, we may be worried that you or someone else is not safe. If we think you might be at risk of harm, we may need to share information with people who can help, for example:

- Social workers
- Safeguarding teams
- The police or other agencies

We will only share information that is needed to help keep you or others safe. We will try to talk to you about this first, unless it is not safe or possible to do so.

How we keep your information safe

We work very hard to keep your information safe. We:

- Use secure computers and passwords
- Make sure only people who need to see your record can see it
- Train our staff so they understand how to keep information private
- Have strict rules and contracts with any other organisations or computer systems that help us

We are not allowed to share your information with people who do not have a good reason to see it.

How long we keep your information

We must keep your health record for a certain amount of time by law. Children's records are normally kept until age 25 (8 years after last treatment if under 18), then reviewed per NHS Records Management Code. When we no longer need your information, it is destroyed safely.

Your rights

Even if you are young, you have rights about your information. You (or your parent or carer, depending on your age and situation) can:

- Ask to see it – This is called a Subject Access Request
- Ask us to fix it – If something is wrong or out of date, you can ask us to correct it.
- Ask questions – You can always ask your doctor, nurse, parent or carer about how we use your information.
- Ask us not to share your information for certain things – For example, some types of research or planning. We cannot always say yes, but we will explain why if we cannot.

From around age 13, you can usually make more decisions about your own health information, but this depends on whether you understand what is involved. Your doctor will talk to you about this.

Online access (NHS App)

From age 11, you might be able to see some of your health record using the NHS App:

- Between ages 11-16, your doctor will check if this is right for you.
- Your parents might be able to see your record too (called "proxy access").
- This will be reviewed regularly, especially at ages 11 and 16, and we may change who can see what, to keep you safe and respect your privacy.

Research and planning

Sometimes we use information about lots of patients together to:

- Plan and improve NHS services
- Check that treatments are working well
- Support medical research

Most of the time this information is anonymised or pseudonymised, which means you cannot be identified. If we ever want to use information that identifies you for research, we will ask for permission from you and/or your parent or carer (depending on your age and understanding), unless the law allows us to use it without consent.

Questions?

If you have any questions about your information or this privacy notice, you can:

- Ask your doctor or nurse
- Talk to your parent or carer
- Ask reception to speak to the Practice Manager

We are here to help and keep your information safe!

How do we maintain the confidentiality of your data?

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

We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

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

All employees and sub-contractors engaged by our Practice are asked to sign a confidentiality agreement. The Practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Charnwood Surgery an appropriate contract will be established for the processing of your information.

Some of this information will be held centrally and used for statistical purposes. Where this happens, we take strict measures to ensure that individual patients cannot be identified.

Sometimes your information may be requested to be used for research purposes. The Practice will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the Practice sharing any of your information for research purposes.

How long do we keep your data?

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 in accordance with National Archives requirements. At the end of these periods, records are securely destroyed in line with NHS policy to ensure confidentiality.

More information on records retention can be found online at [Records Management Code of Practice - NHS Transformation Directorate](#)

What are your data protection rights?

If we already hold your personal data, you have certain rights in relation to it.

Right to object

If we are using your data under **public task** (Article 6(1)(e)), this right has limited application. We will respond to your request within 30 days.

Right to withdraw consent

Where we have obtained your consent to process your personal data for certain activities (for example a research project), or consent to market to you, 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 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply.

Right of data portability

If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP-to-GP data transfer and transfer of your hard copy notes.

National Data Opt-Out

The National Data Opt-Out applies to research/planning (Type 2 objections). We no longer collect Type 1 objections (preventing data leaving for direct care), but you can discuss local preferences with us. You can find out more by visiting [Choose if data from your health records is shared for research and planning - NHS](#).

Who do we share your data with?

We consider patient consent as being the key factor in dealing with your health information. We never sell or monetise your data.

To provide around-the-clock safe care, we will make information available to trusted organisations that are usually independent data controllers (e.g., hospitals, ICBs) for specific purposes unless you have asked us not to.

To support your care and improve the sharing of relevant information to our partner organisations when they are involved in looking after you, we will share information to other systems. The general principle is that information is passed to these systems unless you request that this does not happen, but that system users should ask for your consent before viewing your record.

Our partner organisations are:

- NHS Trusts / Foundation Trusts
- GPs
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups / Integrated Care Boards
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)

- Local Authorities
- Education Services
- Fire and Rescue Services
- Police and Judicial Services
- Other 'data processors' (as detailed in "Our systems and data processors" section)

You will be informed who your data will be shared with, and in cases where your consent is required you will be asked for it.

Below are some examples of when we would wish to share your information with trusted partners.

Primary Care Networks

We are a member of Soar Valley Primary Care Network. This means we work closely with a number of local practices and care organisations for the purpose of direct patient care. They will only be allowed to access your information if it is to support your healthcare needs. If you have any concerns about how your information may be accessed within our primary care network, we encourage you to speak or write to us.

Extended Access

We provide extended access services to our patients which means you can access medical services outside of our normal working hours. In order to provide you with this service, we have formal arrangements in place with the Clinical Commissioning Group and with other practices whereby certain key "hub" practices offer this service on our behalf for you as a patient to access outside our opening hours. Those key "hub" practices will need to have access to your medical record to be able to offer you the service. We have robust data sharing agreements and other clear arrangements in place to ensure your data is always protected and used for those purposes only.

Medicines Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up-to-date and cost-effective treatments. Our local NHS Clinical Commissioning Group employs specialist pharmacists, and they may at times need to access your records to support and assist us with prescribing. The reason for this is to help us manage your care and treatment.

Individual Funding Requests

An Individual Funding Request is a request made on your behalf, with your consent, by a clinician, for the funding of specialised healthcare which falls outside the range of services and treatments that CCG has agreed to commission for the local population. A detailed response, including the criteria considered in arriving at the decision, will be provided to the patient's clinician.

Are there other projects where your data may be shared?

GP Data Sharing Project with NHS East Midlands Ambulance Service

The Practice is working with the local ambulance service trust, NHS East Midlands Ambulance Service, to share your healthcare information for the purposes of your care and treatment. They can only access your information if it is for care purposes. If you have any concerns, please speak to the Practice.

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 admission or re-admission and identifying a need for preventive intervention. Information about you is collected from a number of sources

including NHS Trusts and from this GP practice. A risk score arrived at through an analysis of your de-identified information is provided back to your GP practice 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.

OpenSAFELY

OpenSAFELY is a secure analytics platform used by NHS England and approved academic partners to run large-scale research and analysis on GP records, to help improve NHS services, monitor safety, and plan care.

Data used in OpenSAFELY:

- Is taken from GP systems such as SystmOne in a pseudonymised form (direct identifiers such as your name and NHS number are removed and replaced with codes).
- Never leaves the secure environment controlled for NHS England; approved researchers access data via secure connections and cannot download or remove individual-level data.
- Is used to produce aggregate results and statistics; individual patients are not identified in published outputs.

The legal basis for this use is public task and the provision of health and care services. National data opt-out does not usually apply because data is pseudonymised, but you can discuss any concerns with the Practice if you wish to understand more about how your data may be used in OpenSAFELY.

Research and Planning

We regularly work with local health/academic organisations for research studies and may contact you about participation opportunities (name/contact details only). We always seek consent for identifiable data sharing, except when anonymised. You can opt out of research contact/sharing anytime.

When is your consent not required?

We will only ever use or pass on information about you to others involved in your care if they have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances.

There are certain circumstances where we are required by law to disclose information, for example:

- Where there is a serious risk of harm or abuse to you or other people
- 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

We are also required to act in accordance with Principle 7 of the Caldicott Review (Revised version 2013) which states: "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.

How can you access or change your data?

You have a right under the Data Protection legislation to request access to view or to obtain copies of the information the Practice holds about you and to have it amended should it be inaccurate. Your request should be made to the Practice, and we have a form (SAR - Subject Access Request) which you will need to complete. We are required to respond to you within one calendar month. For information from the hospital, you should write direct to them. You will need to give adequate information (full name, address, date of birth, NHS number and details of your request) so that your identity can be verified and your records located.

There is no charge to receive a copy of the information held about you.

What should you do if your personal information changes?

Please contact the Practice Manager 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). The Practice will from time to time ask you to confirm that the information we currently hold is accurate and up to date.

Changes to our privacy policy

It is important to point out that we may amend this Privacy Notice from time to time. Any changes will be posted on our website and, where appropriate, notified to you by email or at your next appointment.

Our Data Protection Officer

The Practice has appointed **Umar Sabat** as its Data Protection Officer.

He can be contacted by e-mail at umar.sabat@ig-health.co.uk or by calling 07894 826 037.

If you have any concerns about how your data is shared, or if you would like to know more about your rights in respect of the personal data we hold about you, then please contact the Practice Data Protection Officer.

How to contact the appropriate authorities

If you have any concerns about how your information is managed at your GP Practice, please contact the GP Practice Manager or the Data Protection Officer in the first instance.

If you are still unhappy following a review by the GP Practice, you have a right to lodge a complaint with the UK supervisory authority, the Information Commissioner's Office (ICO), at the following address:

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745

Website: [Information Commissioner's Office](https://www.ico.org.uk)

This notice was last updated in March 2026. We review it annually or when significant changes occur.