****

**Cambridge avenue and messingham medical centre**

**GDPR Privacy notice**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| To be reviewed  | Review completed | By | Approved By | Circulation |
| July 2027 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Data Protection Privacy Notice for Patients**

**Introduction:**

This privacy notice explains what happens to any personal data you provide to us, or that we may collect from or about you. It applies to all personal information processed by, or on behalf of, Cambridge Avenue and Messingham Medical Centre.

This notice sets out:

* Who we are, how we use your information, and details of our Data Protection Officer
* What types of personal information we hold and how we use it
* The legal grounds for processing your information (including sharing it with others)
* What to do if your personal information changes
* How long we retain your personal information
* Your rights under data protection law

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) are the primary laws governing how we handle your personal data. These became applicable on 25 May 2018 and, following the UK's departure from the EU, were retained and updated as UK-specific law from 1 January 2021.

For the purposes of data protection legislation (including, but not limited to, Regulation (EU) 2016/679 (the original EU GDPR), the UK GDPR, and the DPA 2018), Cambridge Avenue Medical Centre is the data controller responsible for your personal information.

This notice outlines how we collect, use, and protect your data, and how we meet our legal obligations in doing so. Your privacy matters to us, and we are committed to safeguarding your rights at all times.

**How we use your information and the law.**

Cambridge Avenue and Messingham Medical Centres act as the ‘Data Controllers’ of the personal data you provide. This means we determine how your information is used and are responsible for its security and lawful handling.

We collect standard personal details such as:

* Your name, address, and date of birth
* Contact information including email, mobile number, and home telephone number
* Location-based data where relevant to your care

In addition, we may need to handle more sensitive information — referred to as ‘special category data’ under data protection law. This includes:

* Details about your physical or mental health
* Ethnic background
* Religious beliefs (where relevant in a clinical context)
* Information relating to your sexual orientation or sexual health (if appropriate for your care)

This information may be provided directly by you or shared with us by other health and care professionals involved in your treatment.

**Why do we need your information?**

Our healthcare professionals maintain records about your health and any treatment or care you have received. These records are essential for ensuring you receive the safest, most effective care and treatment possible.

Your NHS health records may be held electronically, or on paper, or in a combination of both. We use secure systems and robust working practices to keep your information confidential and protected.

The types of information we may hold about you include:

* Personal details such as your name, address, carer information, legal representative, and emergency contact
* Records of any contact with the surgery, including appointments, home visits, telephone calls, and clinic attendances
* Notes and reports about your health and medical conditions
* Details of your treatment and any care plans
* Results from investigations such as blood tests, x-rays, and other diagnostics
* Information provided by other health professionals, relatives, or carers involved in your care
* Contact details such as your telephone numbers and email address

Your records support your direct care, including enabling us to contact you when needed. In some cases, limited information may also be used:

* To protect the health of the public
* To support the management and planning of NHS services
* For internal clinical audits to monitor the quality of care we provide

**How do we lawfully use your data?**

As a General Practice, we need to collect and use your personal, sensitive, and confidential information in order to provide you with appropriate healthcare services.

We process your data lawfully under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, based on the following legal grounds:

* 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 (the practice).
* 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 and services.

This privacy notice covers the personal data of our patients, as well as information you may provide to us about your carers or family members.

**We use your personal and healthcare data in the following ways:**

* To communicate with other healthcare professionals — such as doctors, consultants, nurses, or hospital teams — who are involved in your diagnosis, treatment, or ongoing care.
* When we are legally required to share your information with external organisations, such as:
	+ The police (under lawful request)
	+ Courts or solicitors (via court orders)
	+ Government authorities such as immigration enforcement (when legally mandated)
* In a de-identified (anonymous) format to support:
	+ The planning of healthcare services
	+ Improvement of population health outcomes

We will never share your personal information with any third party who does not need it or does not have a legal right to it — unless you give us explicit consent to do so.

**Legal justification for collecting and using your information.**

Under data protection law, we must have a valid legal basis to process your personal and healthcare information. The main justifications we rely on include:

1. **Contract:** We hold a contract with NHS England to provide healthcare services. This contract places a legal obligation on us to deliver care to the public, and this forms a lawful basis for processing your data.
2. **Consent:** In certain situations, we rely on your **explicit consent** to process your personal and healthcare information — for example, when offering services not directly related to essential medical care. You have the right to withdraw your consent at any time if you no longer wish us to process your data in this way.
3. **Necessary care (Vital Interests):** If you are unable to give consent (for example, during a medical emergency), we may process your data in order to protect your vital interests and ensure appropriate care.
4. **Legal Obligation:** Sometimes we are legally required to share your information with other organisations (such as public authorities or law enforcement) where the law demands it.

**Special Category Data**

Health-related data is considered ‘special category personal data’ under the UK GDPR, meaning it is more sensitive and requires additional protection. We may process this data under the following lawful conditions:

* **Public Interest:** When processing your data helps to protect public health — for example, during disease outbreaks or public health emergencies.
* **Consent:** Where you have given explicit permission for us to process your data for a specific purpose.
* **Vital Interests:** If you are unable to consent, and the information is required to protect your life or wellbeing.
* **Defending Legal Claims:** Where the data is necessary to defend a legal claim brought by or against you.
* **Provision of Healthcare:** Where it is required to deliver health or social care services to you.

**Risk Stratification**

At Cambridge Avenue and Messingham Medical Centre, we use risk stratification tools as part of NHS efforts to improve patient care. These tools help identify patients who may be at higher risk of developing certain health conditions or needing emergency hospital care. This allows us to offer preventive support earlier.

To do this, information about you is collected from various NHS sources, including hospital trusts and this practice. Before your data is analysed, any information that identifies you is removed. After analysis, a risk score is created and sent back to your GP in an identifiable form to help us provide personalised care.

The aim is to focus on keeping you healthy and preventing illness, not just treating you when you are unwell. If needed, we may offer you extra services based on this information.

You have the right to opt out of your data being used for risk stratification, except where the law does not allow this. If you wish to opt out or want more information, please contact the practice.

Please note that individual risk management carried out directly by your GP as part of your personal healthcare is not included in this opt-out and is protected by law.

**Anonymised information**

Sometimes, we may share information about you in an anonymised form. This means that all personal details that could identify you are removed. Such information is used to analyse health issues affecting the wider population and helps the NHS plan and improve services.

When your information is shared in this way, it cannot be traced back to you as an individual.

**Medicines Management**

The Practice may carry out Medicines Management Reviews of medications prescribed to patients. These reviews help ensure that you receive the most appropriate, up-to-date, and cost-effective treatments. The reviews are conducted by the Clinical Commissioning Group’s (CCG) Medicines Management Team under a formal Data Processing agreement with the Practice.

**GP Connect Service**

The GP Connect service enables authorised clinical staff at NHS 111 to access our practice’s appointment system securely and book appointments directly on your behalf.

If you contact NHS 111 and the clinician determines you need an appointment with your GP, they will use GP Connect to view available appointment slots and book you in. This saves you time, as you will not need to contact the practice directly to arrange the appointment.

Please be assured that the practice does not share any of your personal data with NHS 111 through this service. NHS 111 can only see available appointment times and will not have access to your medical records. However, any relevant information shared by NHS 111 with the practice about your condition or treatment will be communicated to you.

If you no longer need the appointment or need to change it, please contact the practice reception team directly. NHS 111 cannot make changes to your appointment once it has been booked.

**Summary Care Records**

All patients registered with a GP have a Summary Care Record (SCR) unless they have chosen not to have one. Your Summary Care Record provides registered and regulated healthcare professionals, outside your usual GP practice, with access to essential information to help deliver safer care, reduce the risk of prescribing errors, and improve your overall patient experience.

Your SCR contains basic (Core) information, including details of allergies, current medications, and any past adverse reactions to medicines.

Some patients—particularly those with long-term health conditions—have previously agreed to share Additional Information in their SCR. This may include significant medical history (past and present), reasons for prescribed medications, care plans, and immunisation records.

**Change to information held in your Summary Care Record**

Due to the ongoing COVID-19 pandemic, the Department of Health and Social Care has temporarily removed the requirement for patients’ prior explicit consent to share Additional Information as part of the SCR.

This is because a legal notice issued by the Secretary of State for Health and Social Care requires healthcare bodies to share confidential patient information with other healthcare organisations where necessary to diagnose, control, and prevent the spread of the virus and manage the pandemic. This includes sharing Additional Information through Summary Care Records unless a patient objects.

If you have previously chosen to share only Core information or opted out entirely of having a Summary Care Record, these preferences will continue to be respected and will not be affected by this change.

For all other patients, your Summary Care Record will be updated to include Additional Information for the duration of the pandemic. This temporary change will be reviewed once the current public health emergency has passed.

**Why we have made this change.**

To better support your health and care needs, health and social care organisations may now share your confidential patient information contained in your Summary Care Record with both clinical and non-clinical staff in other healthcare settings, such as hospitals, NHS 111, and out-of-hours services.

These changes are designed to improve the care you receive when you are away from your usual GP practice.

**Your rights in relation to your Summary Care Record**

Regardless of your previous choices about your Summary Care Record, you retain the following options regarding your information:

1. **Full Summary Care Record (Core and Additional Information):**
Authorised, registered, and regulated health and care professionals can access a detailed Summary Care Record containing both Core and Additional Information, if needed to provide you with direct care.
2. **Core Information Only:**
Authorised, registered, and regulated health and care professionals can access only limited information about your allergies and medications in your Summary Care Record, if needed to provide you with direct care.
3. **Opt-Out Completely:**
You can choose not to have a Summary Care Record at all. This means no authorised, registered, or regulated health and care professionals will be able to access your GP-held records to provide direct care, including in emergencies. Please note, if you opt out, you will not be able to change this preference at the time you need urgent care away from your GP practice.

**How to change your Summary Care Record Preferences**

If you wish to update your preferences, please inform your GP practice directly or complete the appropriate form and return it to your GP practice.

**Patient Communication**

Protecting your confidential information is a responsibility we take very seriously. It is therefore essential that you notify us immediately if you change any of your contact details.

We may contact you via SMS text message to your mobile phone to notify you about appointments and other services related to your direct care. To ensure we reach the correct person, please keep your mobile number up to date. This service operates on an ‘opt-out’ basis, which means that by providing us with your mobile number, we assume you consent to receive SMS messages. If you wish to opt out of this service, please inform the practice.

We may also contact you using the email address you have provided. Please ensure your email details are current.

Occasionally, authorised research organisations may invite you to participate in health-related research. Your contact details may be used to send you information about such opportunities.

**Safeguarding**

The Practice is committed to safeguarding adults and children by consistently applying relevant principles and duties, with the wellbeing of all at the core of our work.

Our legal basis for processing your data under the General Data Protection Regulation (GDPR) is as follows:

* **Article 6(1)(e):** *Processing is necessary for the exercise of official authority.*
* **Article 9(2)(b):** *Processing of special category data is necessary for carrying out obligations and exercising specific rights in the fields of employment, social security, and social protection law.*

**Research**

The Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. This data is linked with other health-related information to create a comprehensive, longitudinal dataset representing the UK population’s health. This dataset supports important medical research aimed at improving public health.

You have the right to opt out of your information being used for research purposes at any time. For full details and how to opt out, please visit:
<https://cprd.com/transparency-information>

**Legal basis for Processing Research Data**

While CPRD does not hold or process identifiable patient data, NHS Digital (formerly the Health and Social Care Centre) may process personal data on behalf of CPRD as an accredited ‘safe haven’ or ‘trusted third party’ within the NHS. This processing is necessary to link 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) — *processing is in the public interest for public health purposes.*
* **Medical research and statistics:**
Article 6(e) and Article 9(2)(j) — *processing is in the public interest and for scientific research purposes.*

All data held or shared by CPRD for research (except in clinical research studies) is anonymised in accordance with the Information Commissioner’s Office Anonymisation Code of Practice.

CPRD retains data indefinitely to support future research, though individual research studies typically hold released data for no longer than twelve months.

**Categories of Personal Data Collected in Safeguarding Situations**

In safeguarding cases, Cambridge Avenue and Messingham Medical Centre will collect as much personal information as necessary to effectively manage the situation. This may include basic demographic and contact details, as well as details about the safeguarding concern. Such information often includes special category data, such as health information, and is processed with appropriate safeguards in place.

**Sources of the data**

The Practice collects or receives information when someone contacts us with safeguarding concerns, or when we identify potential safeguarding issues and make enquiries to relevant healthcare or social care providers.

**Recipients of personal data**

Information collected is used by the Practice to manage safeguarding incidents or concerns. We may share this information, as necessary, with partner organisations such as local authorities, the police, or other healthcare professionals involved in your care (e.g., your GP or mental health team) to ensure your safety and wellbeing.

**Third party processors**

To provide the best possible care and service, the Practice may share data with other NHS bodies, such as other GP practices or hospitals. Additionally, we use carefully selected third-party service providers who process data on our behalf.

Before sharing data, we ensure there is a formal agreement in place to guarantee that:

* Your data is kept secure.
* Data is only used or shared according to our instructions.
* The third party complies with relevant data protection laws.

Examples of such third-party services include:

* IT service providers supporting clinical systems, patient-facing websites, appointment booking, electronic prescriptions, and document management.
* Delivery services, for example, if we arrange medication deliveries.
* Payment providers, for example, when paying for prescriptions or services like travel vaccinations.

If you would like more information about specific third-party processors, please contact our Data Protection Officer (details below).

**How do we maintain the confidentiality of your records?**

We are committed to protecting your privacy and handling your information lawfully in accordance with the following:

* Data Protection Act 2018
* General Data Protection Regulation (GDPR) 2016
* 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”

Every member of NHS staff has a legal duty to keep your information confidential. We will only use or share your information if it is necessary for your care or with your permission.

In exceptional circumstances, such as life-threatening situations or where the law requires, we may share information without your consent. Following the Caldicott principles, health and social care professionals are encouraged to share information appropriately in the best interests of patients while maintaining confidentiality.

Our practice policy respects the privacy of patients, families, and staff and complies fully with GDPR and all UK data protection laws.

All staff and subcontractors working with the Practice sign confidentiality agreements. Where subcontractors act as data processors on behalf of Cambridge Avenue Medical Centre, appropriate data processing contracts (Articles 24-28 GDPR) are in place.

**Your Rights and Data Retention**

You have the right to withdraw your consent to data processing at any time by contacting our Data Protection Officer in writing. In some cases, we may need to retain your data even after consent is withdrawn to comply with legal obligations.

Some data is held centrally for statistical purposes, with strict measures in place to ensure individuals cannot be identified.

If your information is requested for research, the Practice will seek your consent before sharing any identifiable information. You also have the option to opt out of your data being used for research purposes.

**Using your information with your consent**

Sometimes, we may want to use your information to contact you about services that are not directly related to your healthcare. Before doing so, we will always ask for your consent. With your permission, we would like to use your name, contact details, and email address to inform you about other services that may benefit you. We will only contact you if you agree to this.

Occasionally, authorised research organisations may invite you to take part in innovations, research projects, service improvements, or to help identify health trends. You will always be asked to opt in before participating in any such programme. If we want to use your data for any purpose outside those already specified, and where there is no legal requirement to share or process your data, we will always seek your consent and provide you with the option to opt out before processing begins.

We do not share this information with third parties for marketing purposes. You can unsubscribe at any time by contacting us via phone, email, or by informing the practice’s Data Protection Officer (DPO) as shown below.

**National Opt-Out Facility**

You have the right to choose whether your confidential patient information is used for research and planning purposes.

**Who uses your information for research and planning?**

Your information may be used by the NHS, local authorities, university and hospital researchers, medical colleges, and pharmaceutical companies working on new treatments.

**How to make your opt-out choice:**

You can opt out of sharing your confidential patient information for research and planning purposes. However, in some situations—such as during an epidemic—your information might still be used to protect public health.

Opting out will not affect the care or treatment you receive. You will still be invited to attend screening services (for example, bowel cancer screening).

If you are happy with how your data is used, you do not need to take any action.

To opt out securely or find out more, visit [nhs.uk/your-nhs-data-matters](https://www.nhs.uk/your-nhs-data-matters) or call 0300 303 5678. You can change your choice at any time.

**NHS Digital Data Collection from the Practice**

NHS Digital collects patient data from GP practices to help plan and deliver safe, effective healthcare services for everyone. This programme, called General Practice Data for Planning and Research (GPDPR), supports:

* Monitoring long-term safety and effectiveness of care
* Planning better health and care services
* Preventing the spread of infectious diseases
* Identifying new treatments through health research

GP practices already share data for these purposes, but this new collection will make the process more efficient.

NHS Digital works with professional bodies like the British Medical Association and Royal College of GPs to ensure patient safeguards are in place.

What data NHS Digital collects

Starting 1 July 2021, NHS Digital will collect data about:

* All living patients registered with GP practices in England
* Patients who have died since the data collection started

The data collected will not include your name or address. Identifiers like NHS number and date of birth are replaced by unique codes through a process called pseudonymisation, ensuring you cannot be directly identified.

NHS Digital is the only organisation with the legal ability to re-identify data in limited, lawful circumstances—for example, if you consent to identifiable data being shared with a research project you are participating in.

Opting out and data protections:

* You do not need to register a Type 1 opt-out by 1 September to prevent your GP data being shared.
* NHS Digital will allow deletion of previously shared data if you register a Type 1 opt-out later.
* Plans to retire Type 1 opt-outs are deferred until proper arrangements are in place, following consultation with medical and data guardian organisations.

For more details about how your data is used and protected, and to exercise your rights, please visit the NHS Digital website or contact your GP practice.

**What data NHS Digital collects**

* NHS Digital collects structured and coded data from your GP medical records needed for specific health and social care purposes.
* Personal identifiers like your NHS number, GP patient number, full postcode, date of birth, and date of death (if relevant) are replaced with unique codes by special software before data is sent to NHS Digital. This process ensures no one can directly identify you from the data.
* NHS Digital can re-identify data in very limited circumstances where there is a valid legal reason (for example, if you consent to participate in a clinical trial). Even then, your data remains securely protected.

**Examples of Data Collected by NHS Digital:**

* Your sex, ethnicity, and sexual orientation
* Clinical information including diagnoses, symptoms, test results, medications, allergies, immunisations, referrals, recalls, and appointments (covering physical, mental, and sexual health)
* Data about healthcare staff who have treated you

**What NHS Digital Does Not Collect:**

* Your name and address (except for postcode in coded form)
* Written notes such as doctors’ and nurses’ free text entries
* Images, letters, and documents
* Old coded data not needed for current care (e.g., medication or referral data over 10 years old)
* Certain sensitive data that GPs are not legally allowed to share (e.g., IVF treatment codes, some gender reassignment information)

**Opting Out of NHS Digital Data Collection (Type 1 Opt-out)**

* You can tell your GP practice that you do not want your identifiable patient data shared outside the practice for purposes beyond your own care. This is called a Type 1 Opt-out.
* Type 1 Opt-outs have been in place since 2013, but may be phased out in future as a new National Data Opt-out (which covers a wider range of health and care data) becomes standard. If this changes, you will be informed.
* NHS Digital will not collect your data if you have a valid Type 1 Opt-out registered.
* You can register or withdraw a Type 1 Opt-out at any time by contacting your GP practice or calling 0300 303 5678.
* Data sharing with NHS Digital began on 1 September 2021.
* If you register a Type 1 Opt-out after your data has already been shared, no new data will be shared, but NHS Digital will still hold previously shared data.

**Legal Basis for NHS Digital’s Data Collection and Sharing**

* NHS Digital collects and processes data under strict legal rules, including the UK General Data Protection Regulation (GDPR) and the Health and Social Care Act 2012.
* The Secretary of State for Health and Social Care has issued specific directions for NHS Digital to collect data for planning, research, public health, and policy.
* NHS Digital works with independent groups and follows robust oversight to protect your data.
* During public health emergencies like COVID-19, additional legal notices allow sharing confidential data to protect public health; this use is limited to the emergency period unless other laws apply.

**How NHS Digital Uses Patient Data**

* NHS Digital analyses and links data to create national datasets and improve data quality.
* Re-identification of coded data is only possible under strict controls, with legal and ethical approval, for reasons such as:
	+ Providing care to you
	+ Your explicit consent (e.g., clinical trials)
	+ Legal obligations (such as public health emergencies)
	+ Regulatory approvals (e.g., by Health Research Authority)
* All published data is anonymous and cannot identify you.

**Who NHS Digital Shares Data With**

* Data is only shared when necessary and with organisations that have a legal basis to use it, such as:
	+ Department of Health and Social Care and agencies (e.g., Public Health England)
	+ NHS England and NHS Improvement
	+ Primary care networks, clinical commissioning groups, integrated care organisations
	+ Local authorities
	+ Approved research organisations (universities, charities, clinical trials, pharmaceutical companies)
* Access to identifiable data requires strict approvals, data sharing agreements, and oversight by independent advisory groups.
* Data is shared in a de-personalised form by default and only re-identified where legally justified and with your consent where required.
* If you have registered a National Data Opt-out, it will be applied to prevent sharing your identifiable data beyond your own care.

**More Information**

* For full details on data shared, visit NHS Digital’s Data Release Register online.
* To register or manage your opt-outs, visit [nhs.uk/your-nhs-data-matters](https://www.nhs.uk/your-nhs-data-matters) or call 0300 303 5678.

**Where NHS Digital Stores Your Patient Data**

* NHS Digital only stores and processes patient data within the United Kingdom (UK) for this data collection.
* Fully anonymous data (which cannot identify you at all), such as published statistical information, may be stored and processed outside the UK.
* Some third-party processors may process patient data outside the UK, but only when strict data protection laws are followed to keep your data safe.

**Electronic Storage of Your Data**

* All personal data is handled by NHS Digital staff within the UK.
* For IT hosting and maintenance, some data may be stored on servers located in the European Union (EU).
* No third parties have access to your personal data unless:
	+ The law allows it, and
	+ Proper safeguards, such as Data Processing Agreements, are in place.
* NHS Digital has strong data protection policies to ensure your information is processed securely and responsibly.

**Who NHS Digital May Share Your Data With**

Your information may be shared, under strict agreements and controls, with the following types of organisations:

* NHS Trusts and Foundation Trusts
* General Practitioners (GPs)
* Primary Care Networks (PCNs)
* NHS Commissioning Support Units
* Independent contractors like dentists, opticians, pharmacists
* Private sector providers
* Voluntary sector providers
* Ambulance Trusts
* Clinical Commissioning Groups (CCGs)
* 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
* Yorkshire & Humber Care Record system
* Healthy.io (for specific patient programmes)
* Other approved ‘data processors’ (you will be informed about these)

You will be informed about who your data is shared with and, when required, asked for your consent.

**Clinical Computer Systems and Data Sharing**

* The GP practice uses a secure clinical computer system where NHS staff record your medical information.
* This information can be shared with other healthcare professionals involved in your care to provide the best treatment.
* To support safe care 24/7, your information will be made available to trusted organisations unless you ask us not to.
* Wherever possible, staff will ask for your consent before viewing your information.

**The Yorkshire & Humber Care Record**

* This is a shared system used by healthcare staff across the Humber, Coast, and Vale area.
* It allows staff to access the most up-to-date information about you to provide the best possible care.
* The Yorkshire & Humber Care Record Guarantee commits to using your records respectfully and to promote your health and wellbeing.
* If you want more information or have questions, please contact our Data Protection Officer (details provided by your practice).

**ACR Project for Patients with Diabetes**

* NHS Digital sponsors a programme to help monitor kidney health in patients at risk of chronic kidney disease (CKD), such as those living with diabetes.
* The programme enables you to test your kidney function at home by sending a test kit.
* Your contact details may be shared with Healthy.io, the company delivering this service, who will contact you to arrange sending a kit.
* Healthy.io will only use your data to provide this testing service.
* If you prefer not to receive a home test kit, your care will continue as usual at the GP practice.
* Healthy.io follows strict rules about data retention and protection (more info: <http://bit.ly/uACRtest>).

**Shared Care Records and Data Sharing**

* To improve your care, your medical information may be shared with partner organisations involved in your treatment.
* Information is generally shared unless you ask us not to, but those who access your records should ask for your consent before viewing.
* Sometimes, external companies may process your data (e.g., for archiving). These companies must keep your information confidential and secure by law and contract.
* All staff and subcontractors working with the practice must sign confidentiality agreements, and any subcontractors acting as data processors have formal contracts to protect your data.

**Sharing Your Information Without Consent**

Although we usually ask for your consent, there are situations when the law requires us to share your information without your consent, such as:

* Serious risk of harm or abuse to you or others
* Safeguarding investigations
* Serious crime investigations or prevention
* Notification of new births
* Infectious diseases that could threaten others (e.g., meningitis, measles—but not HIV/AIDS)
* Formal court orders
* Legal requirements, like road traffic offenses

**How Long We Store Your Information**

* We keep your records as required by UK law and NHS Records Management Code of Practice.
* For more details, see: [Records Management Code of Practice for Health and Social Care](https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016)

**Your Rights Regarding Your Data**

You have rights about the personal data we hold:

* Right to object: If we process your data based on our legitimate interests and you disagree, you can object. We will respond within 30 days.
* Right to withdraw consent: If you gave consent for specific uses (e.g., research), you can withdraw it anytime.
* Right to erasure (“right to be forgotten”): In some cases, you can ask us to delete your data. We’ll respond within 30 days and may keep a record to avoid future contact if you prefer.
* Right of data portability: You can ask us to transfer your data to another provider, such as for GP-to-GP transfers.

To exercise your rights or ask questions, please contact us.

**Primary Care Networks (PCNs)**

* PCNs are groups of GP practices working together to improve patient care and support staff.
* By June 2019, most areas in England are covered by PCNs serving 30,000–50,000 patients.
* PCNs help practices share resources, offer more services, and work with wider health and social care systems.
* Your information may be shared within your PCN to support your care and treatment.

**Population Health Management (PHM) Pilot Project**

* PHM aims to improve the health of entire communities by sharing data between healthcare organisations and partners.
* This pilot is running in Derby and Derbyshire and involves GP practices and other care providers.
* Your identifiable personal data is replaced with a code to keep you anonymous.
* If extra care or support might benefit you, coded info is sent back to your GP or hospital to identify you and offer help.
* Your health info is securely shared with the North of England Commissioning Support Unit (NECS) and their partner Optum, both legally required to keep it confidential.
* PHM is lawful under data protection laws for medical care and service management.
* The project lasts 22 weeks; after that, all de-identified data will be securely destroyed.
* This will not affect any personal data your GP or other providers hold.

More info:

* NECS: <https://www.necsu.nhs.uk>
* Optum: [www.optum.co.uk](http://www.optum.co.uk)

**Access to Your Personal Information**

**Your Rights**

* You can ask to see or get a copy of the personal information the practice holds about you.
* You can also ask for corrections if any information is inaccurate.
* To make a request (called a Data Subject Access Request or DSAR):
	+ Contact the practice directly (for hospital records, contact them separately).
	+ There is no charge for this.
	+ We must respond within one month.
	+ You’ll need to provide enough details to verify your identity (name, date of birth, NHS number, etc.).

**Keeping Your Details Up to Date**

* Please let us know if your personal information changes, especially your address or phone number.
* The practice will occasionally ask you to confirm your details are current.

**Online Access to Your Medical Records**

* You can request online access to your medical record.
* You’ll need to give complete the form at reception and prove your identity.
* Once given, it’s your responsibility to keep your login details secure and prevent others from accessing your information.

**Information About Third Parties**

* Sometimes your medical record mentions other people (third parties).
* We protect their privacy by removing or redacting any confidential info about them before sharing your record.

**CCTV at the Practice**

* CCTV covers external and internal areas (except consulting rooms).
* It is used to improve security and prevent crime.
* Recordings are password protected and overwritten regularly.

**Telephone Recordings**

* Calls to the practice are recorded and stored for up to three years.
* Recordings help resolve disputes and are used for staff training.
* Access is restricted to senior staff.

**Medical Examiner Service**

* After a patient’s death, the practice must inform the Medical Examiner Service.
* Medical Examiners review non-coronial deaths, offer families a chance to ask questions, and ensure the cause of death is properly recorded.
* The practice will share patient details with the service when requested.

**Objections & Complaints**

* If you have concerns about how your data is managed, contact the Practice Manager or the Data Protection Officer.
* If unsatisfied, you can complain to the UK Information Commissioner’s Office (ICO):

**Information Commissioner’s Office+-**
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Phone: 01625 545745
Website: [ico.org.uk](https://ico.org.uk/)

**Contacting the Data Protection Officer**

For any questions about your data or this Privacy Notice:

**Paul Couldrey, Data Protection Officer**
Email: paul.couldrey@nhs.net

**Changes to This Privacy Notice**

* We may update this Privacy Notice from time to time.
* If you have concerns about changes, please contact the Data Protection Officer.

**Published:** May 2018
**Last Reviewed:** July 2025