

Cofton Medical Centre (the Practice)
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 the practice.

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 should you do if your personal information changes?
- For how long your personal information is retained / stored by us?
- What are your rights under Data Protection laws

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) became law on 25th May 2018. The GDPR is a single EU-wide regulation on the protection of confidential and sensitive (special) information, the DPA 2018 deals with elements of UK law that differ from the European Regulation, both came into force in the UK on the 25th May 2018, repealing the previous Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 the practice responsible for your personal data is Cofton Medical Centre.

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.

How we use your information and the law.

Cofton Medical Centre will be what's known as the 'Controller' of your personal data.

We collect basic personal data about you and location-based information. This does include name, address and contact details such as email and mobile number etc.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious belief (if required in a healthcare setting) ethnicity and sex life information that are linked to your healthcare, we may also receive this information about you from other health providers or third parties.

Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

NHS health records may be electronic, paper-based or a mixture of both. We use a combination of working practices and technology to ensure that your 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 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, including 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 within the GP practice for clinical audit to monitor the quality of the service we provided.

How do we lawfully use your data?

We need your personal, sensitive and confidential data in order to provide you with healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with: -

Article 6, 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, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

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

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 this GP Practice. 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 the practice for further information about opt out.

Individual Risk Management at a GP practice level however is deemed to be part of your individual healthcare and is covered by our legal powers above.

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. The reviews are carried out by the CCGs Medicines Management Team under a Data Processing contract with the Practice.

Patient Communication

The Practice will like to use your name, contact details and email address to inform you of NHS services, or provide inform about your health/information to manage your healthcare or information about the management of the NHS service. There may be occasions where authorised research facilities would like you to take part in research in regard to your particular health issues, to try improve your health., Your contact details may be used to invite you to receive further information about such research opportunities.

Safeguarding

The Practice 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 For the General Data Protection Regulation (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...’

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 Digital (formally the Health and Social Care 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.

Categories of personal data

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is possible that 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 Practice 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 by the Practice 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).

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice 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 & 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 do 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 General Data Protection Regulations 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 Review

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

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 practice policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the General Data Protection Regulation (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 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 Cofton Medical Centre 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. If 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 – the 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 the surgery sharing any of your information for research purposes.

With your consent we would also like to use your 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 practice DPO as below.

National Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning.

Who can use your confidential patient information for research and planning?

It is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

Making your data opt-out choice

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used: for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Will choosing this opt-out affect your care and treatment?

No, your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services, such as screenings for bowel cancer.

What should you do next?

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt out securely online or through a telephone service.

You can change your choice at any time. To find out more or to make your choice visit nhs.uk/your-nhs-data-matters or call 0300 303 5678

Where do we store 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.

No 3rd 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.

EMIS Web

The Practice uses a clinical system provided by a Data Processor called EMIS, with effect from 10th June 2019, EMIS will start storing your practice's EMIS Web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services ("AWS").

The data will remain in the UK at all times and will be fully encrypted both in transit and at rest. In doing this, there will be no change to the control of access to your data and the hosted service provider will not have any access to the decryption keys. AWS is one of the world's largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the very highest levels of security and support.

Who are our partner organisations?

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
- GP's
- Primary Care Network
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- 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

This practice operates 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 Organisation (above). Wherever possible, their staff will ask your consent before your information is viewed.

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 anytime 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 by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for Cofton Medical Centre an appropriate contract (art 24-28) will be established for the processing of your information.

Birmingham and Solihull Shared Care Record

Cofton Medical Centre works with other health and social care organisations to share information that will form part of your Shared Care Record. The Shared Care Record allows health and care professionals involved in your care to view your records to help them understand your needs and make the best decisions with you, and for you. Information we hold about you will be available, to read only, to other health and care professionals in Birmingham and Solihull, Coventry and Warwickshire, and Herefordshire and Worcestershire when they are involved in your health or social care.

For more information on how your data is used on the Shared Care Record and how to exercise your rights please see the full [Privacy Notice](https://www.livehealthylivehappy.org.uk/birmingham-and-solihull-shared-care-record/privacy-notice/) or copy and paste this link: www.livehealthylivehappy.org.uk/birmingham-and-solihull-shared-care-record/privacy-notice/.

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://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>).

How can you access, amend move 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 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 consent to send 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. We will help with this with a GP to GP data transfer and transfer of your hard copy notes.

Primary Care Network

The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces which ease the pressure of GP's, leaving them better able to focus on patient care. The aim is that by July 2019, all areas within England will be covered by a PCN.

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

All GP practices are expected to come together in geographical networks covering populations of approximately 30–50,000 patients by June 2019 if they are to take advantage of additional funding attached to the GP contract. This size is consistent with the size of the primary care homes, which exist in many places in the country, but much smaller than most GP Federations.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Access to your personal information

Data Subject Access Requests (DSAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery 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 Practice. (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 information we hold about you at any time.

Digitisation of Paper Medical Records – Privacy Notice

The NHS Long Term plan published in 2019 requires the digitisation of all primary care paper medical records, commonly known as ‘Lloyd George’ records or ‘A4 medical records’

Having paper based medical records restricts the use of technology to provide ‘joined up’ services and therefore the current paper records will be transferred to a digital format and then destroyed.

This will involve the current patient paper medical records being scanned and then entered directly into a patient’s electronic medical record. This work will be completed by a third party supplier, Northgate Public Services, whose security standards have been reviewed by NHS Birmingham and Solihull Clinical Commissioning Group.

We are required by Data Protection law to provide you with the following information about how we handle your information.

Data Controller contact details	Cofton Medical Centre, 2 Robinsfield Drive, West Heath, Birmingham, B31 4TU
Data Protection Officer contact details	Name: SDS MyHealthcare Email: sdsmyhealthcare.ig@nhs.net Postal: West Heath Medical Centre 194-196 West Heath Road West Heath Birmingham B31 3HB
Purpose of the processing	Transferring the current paper medical records into patients’ electronic medical records.

Lawful basis for processing	<p>The following provisions of the General Data Protection Regulation permit us to digitise existing paper medical records:</p> <p>Article 6(1)(e) – ‘processing is necessary...in the exercise of official authority vested in the controller...’</p> <p>Article 9(2)(h) – ‘processing is necessary for the purpose of preventative...medicine...the provision of health or social care or treatment or the management of health or social care systems and services...’</p>
Recipient or categories of recipients of the processed data	The paper patient records will be shared with Northgate Public Services, who will scan and digitise the current paper medical records before destroying them.
Right to access and correct	You have the right to access your medical record and have any errors or mistakes corrected. Please speak to a member of staff or look at our ‘subject access request’ policy on the practice website.
Retention period	<p>GP medical records will be kept in line with the law and national guidance. Information on how long records can be kept can be found at: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016 or speak to the practice.</p> <p>The paper medical records will be destroyed three months after they are transferred to an electronic format.</p>

The practice holds medical records to provide medical treatment and advice and patients have a relationship with a GP in order for them to be providing health and care service to you. We therefore do not require your consent to transfer these papers records to an electronic format.

If you have any questions about this project, please contact Cofton Medical Centre.

Details of Supplier

Northgate Public Services

Queens Court
Wilmslow Road
Alderley Edge
Cheshire
SK9 7RR
www.northgatepublicservices.com

GP Connect Privacy Notice

We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patients care, leading to improvements in both care and outcomes.

GP Connect is not used for any purpose other than direct care.

Authorised Clinicians such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect.

The NHS 111 service (and other services determined locally e.g. Other GP practices in a Primary Care Network) will be able to book appointments for patients at GP practices and other local services.

Legal basis for sharing this data

In order for your Personal Data to be shared or processed, an appropriate “legal basis” needs to be in place and recorded. The legal bases for direct care via GP Connect is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider:

- for the processing of personal data: Article 6.1 (e) of the UK GDPR: “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”.
- for the processing of “Special Category Data” (which includes your medical information): Article 9.2 (h) of the UK GDPR: “processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services”.

Your rights

Because the legal bases used for your care using GP Connect are the same as used in other direct care situations, the legal rights you have over this data under UK GDPR will also be the same- these are listed elsewhere in our privacy notice.

Find [out more about GP Connect](#).

Summary Care Record Privacy Notice

During the height of the pandemic changes were made to the Summary Care Record (SCR) to make additional patient information available to all appropriate clinicians when and where they needed it, to support direct patients care, leading to improvements in both care and outcomes.

These changes to the SCR will remain in place, unless you decide otherwise.

Regardless of your past decisions about your Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

You can exercise these choices by doing the following:

1. **Choose to have a Summary Care Record with all information shared.** This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.
2. **Choose to have a Summary Care Record with Core information only.** This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your Summary Care Record if they need to provide you with direct care.
3. **Choose to opt-out of having a Summary Care Record altogether.** This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

To make these changes, you should inform your GP practice or complete this [form](#) and return it to your GP practice.

Legal basis for sharing this data

In order for your Personal Data to be shared or processed, an appropriate 'legal basis' needs to be in place and recorded. The legal bases for direct care via SCR is the same as the legal bases for the care you would receive from your own GP, or another healthcare provider:

- for the processing of personal data: Article 6.1 (e) of the UK GDPR: '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'.
- for the processing of 'Special Category Data' (which includes your medical information): Article 9.2 (h) of the UK GDPR: 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'.

Your rights

Because the legal bases used for your care via SCR are the same as used in other direct care situations, the legal rights you have over this data under UK GDPR will also be the same- these are listed elsewhere in our privacy notice.

[Find out more about SCR.](#)

General Practice Data for Planning and Research (GPDPR) Data Collection

The purpose of the data collection is to support the provision of general practice data for planning and research.

All GP practices in England are legally required to share data with NHS Digital for this purpose under the Health and Social Care Act 2012 (2012 Act). More information about this requirement is contained in the [data provision notice issued by NHS Digital to GP practices](#).

You have the choice to opt out if you wish to you need to complete the opt out form (available from the practice or on our website) and send this to your Practice. You can learn more about how NHS Digital uses your data here: [General Practice Data for Planning and Research: GP Practice Privacy Notice - NHS Digital](#)

Privacy Notice about Locality Hubs

As you are registered as a patient of this GP practice we collect and use information about you (“**personal data**”).

Starting in Winter 2023 we are working alongside other GP practices in the locality, to run Locality Hubs. This section of the Privacy Notice tells you about the special ways that we use your personal data so we can help to run the Locality Hubs.

Who are your controllers?

A controller is an organisation that uses your personal data and decides their purposes and methods for using it.

This GP practice is a controller of information about your health and healthcare. Our general purposes for using your personal data are described in our patient Privacy Notice. We are still your GP practice, but we get (and contribute to) some extra help over the Locality.

For the Locality Hubs, this practice is collaborating with other local GP practices to handle appointments for you during the winter rush, when we will get busy. Each of the GP practices that we work with will also become a controller of your personal data, just so they can help us run the Locality Hub. We’re doing the same for their patients, too. The GP practices are:

- College Green Medical Practice
- West Heath Surgery

Together, these GP practices are ‘joint controllers’ in relation to Locality Hubs. This means that we make the decisions *together*, as a group of practices. None of the practices can make decisions about the use of your personal data on their own. So we, your ‘home’ practice, are always involved.

Who are the data protection officers?

You should carry on using our data protection officer as your main point of contact.

Each of the GP practices listed above has an officer who is responsible for that practice’s use of personal data. If a data protection officer from any of the other practices is needed, our data protection officer will involve them.

What personal data will you use, and what will you do with it?

The Locality Hub will provide extra facilities between January and the end of June. When you request an appointment with us during that period, we may offer you the appointment at the Locality Hub, and then your appointment could be with any GP from any of the practices listed above. Here is a list of the facilities and what this means for your personal data:

- *Locality Hub online booking/ cancellation website/app* We access the website/app to book Locality Hub appointments: it is not available for you to book. 111 can also access it for you, too. All of the practices can see your appointment on the Locality Hub. Any of the practices can accept your appointment request.

- *Locality Hub appointments* Your appointment is with a GP at the practice that accepts your appointment. The clinician who takes your appointment will have access to the health records that we hold about you. The GP has access to, but cannot edit, your health records.
- *Locality Hub appointment reminders* A reminder will be sent to you via SMS. The reminder is sent to you by the Locality access hub following a booking by your practice or 111.
- *Locality Hub prescriptions* The clinician who takes your appointment can make an electronic prescription for you.
- *Locality Hub appointment notes* The clinician who takes your appointment will keep their own notes about the appointment and any prescriptions, tests requested, and referral to any Consultant, and will share these with us electronically (via the Locality Hub)* so we can include them in the health records that we hold about you.
- *Locality Hub identity checks* The booking website/app and each clinician and GP practice needs to be able to check who you are, to manage appointment booking and attendance. We allow the Locality Hub website/app and attendance IT systems to look up your name, address and data of birth from the NHS Patient Demographic Service*.
- *Locality Hub test results* The clinician who takes your appointment submits the test via the Locality Hub and the results come electronically (via the Locality Hub)*, so we can include both the request for the test and the results in the health records that we hold about you. The clinician who takes your appointment will also keep a copy for their own records.
- *Locality Hub referrals* The clinician who takes your appointment initiates the referral to a Consultant via the Locality Hub*, so we can log it in the health records that we hold about you. The clinician who takes your appointment will also keep a copy for their own records.
- *Website/app and electronic hub* One of the practices runs the booking website and other connecting technology to form the Locality Hub, for the other practices. It might need to use your personal data to set up the portal and hub, and to fix them (if they go wrong)*.
- *Management reporting* The GP practices will keep statistics and similar non-personal information to help them and NHS Birmingham & Solihull Integrated Care Board to manage the Locality Hub. This will include the number of appointments booked on Locality Hub, the types of appointment, the role of the clinician who took the appointment, and who booked (your 'home' practice or 111). This information is not personal data, but we and the other GP practices need to use your personal data to get it.

Your choices about use of your personal data for the Locality Hub

If you do not use the Locality Hub, we will not share your health records with the Locality Hub. Clinicians at the other practices can only access the health records that we hold about you if they take an appointment with you.

All of the practices need access to your identity information: that's how the portal confirms who you are, and how we manage bookings and attendance for the Locality Hub. So, unless you tell us you will never use the Locality Hub and you want to opt out, we will make that information available to the Locality Hub. If you do not take an appointment with a clinician from another practice, the other practices will not have access to this information.

What we will not do with your personal data

We have all read stories of how data is misused by Big Tech. None of the GP practices running the Locality Hub will be allowed to use your personal data for their own purposes, or to share it for

research, or to sell it. They will only be allowed to use it as described above, so we can run the Locality Hub for you.

Lawful basis

The lawful basis that the GP practices jointly rely on for using your personal data for the Locality Hub is: the use is necessary for the performance of a task carried out in the public interest. (This lawful basis is set in Article 6(1)(e) of UK GDPR.) It is necessary because a lone GP practice may run out of appointments on some days during the Winter. That is less likely to happen if we combine resources.

Special category data

Your health records that we hold might include 'special category data', such as information about your health, race or ethnicity, or sex life or orientation. (If you are not sure what 'special category data' means, see our general patient Privacy Notice, which tells you.)

By law, the GP practices listed above can only use your 'special category data' for limited purposes. The purpose that they rely on for the Locality Hub (including keeping and sharing Locality Hub appointment notes for your 'home' practice) is: the use is necessary for the provision of health care or treatment or the management of health care systems and services. (This permission is set in Article 9(2)(h) of UK GDPR.)

If a different GP practice (not your 'home' practice) takes your appointment, the purpose that they rely on for keeping their appointment notes and any prescriptions, tests requested, and referral to any Consultant is: the use is necessary for establishing, exercising or defending legal claims. (This permission is set in Article 9(2)(f) of UK GDPR.)

Who else will the GP practices share your personal data with?

The Locality Hub uses computer technology to share your personal data between the GP practices. In the description of how we use your personal data for the Locality Hub (above), an asterisk (*) marks pieces of technology that we rely on. The supplier names or types for the Locality Hub are:

- Providers of software (and related services) for keeping electronic patient records.
- NHS Digital. It operates the NHS Spine (which NHS organisations use to share patient personal data electronically), the Personal Demographics Service (a national database of patient identifying details), and GP Connect (which the GP practices use to connect with the computer hubs to share your personal data and receive appointment notes back).
- Providers of online booking software or services, or booking apps for your phone or tablet. (We will give you separate instructions about how to book Locality Hub appointments.)
- NHS Birmingham & Solihull Integrated Care Board, which supports the GP practices generally with building the technology for Locality Hub.
- Broadband providers.

The suppliers may come into contact with your personal data, but it only happens if it's unavoidable for the suppliers to do their jobs, such as setting up the portal, hubs or interconnections, or diagnosing and fixing them (if they go wrong).

None of the suppliers is allowed to access your personal data except with the permission of the GP practice they work for, and they will never be given permission to use your personal data for their own purposes.

This notice is only about the Locality Hub. As your GP practice, we use other suppliers besides those listed above. See our general patient Privacy Notice for more information.

How long will we keep your information?

As your 'home' practice, we keep your personal data for as long as you are registered as our patient: see our general patient Privacy Notice.

If a different GP practice (not your 'home' practice) takes your appointment, it will keep its appointment notes in accordance with the NHS records retention policy.

Your rights

You have the following rights in relation to the personal data that is used for the Locality Hub:

- Get access to your personal data.
- Correction of your personal data.
- Erasure of your personal data. (This right only applies in limited circumstances, though, and in the context of the Locality Hub it will not normally apply.)
- Restriction on the use of your personal data, in limited circumstances.
- Object to the use of your personal data based on your particular circumstances. If you raise an objection, we and the other GP practices may continue to use your personal data to establish, exercise or defend legal claims, and in some other cases too.
- Object to the use of your personal data for marketing, and require it to stop. Appointment SMSs are reminders about an appointment that you have made, and are not marketing.
- Not to be subject to decisions made by computers 'drawing inferences' and making significant decisions about you. The connecting hubs and the appointment website/app do not use automated decision-making. Checking your identity is based on facts, not inferences.]
- Complain to the Information Commissioner.

If you want to exercise any of your rights, please contact this GP practice (your 'home' practice). Although the GP practices for the Locality Hub are joint controllers, we are best placed to understand and respond to your requests, and it will be difficult (and may be impossible) for the other practices. You can contact us as follows:

0121 693 5777, Coftonmedical.centre@nhs.net or 2 Robinsfield Drive, West Heath, Birmingham, B31 4TU

If you need this document in large print or braille or in a different language, or you need help understanding the document, please contact coftonmedical.centre@nhs.net

If you have given us information about someone else, such as your next of kin or an emergency contact, please give this notice to that person. It affects them as well as you.

What should you do if your personal information changes?

You should tell us so that we can update our records 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.

Objections / Complaints

Should you have any concerns about how your information is managed at the GP, please contact the GP Practice Manager or the Data Protection Officer as above. If you are still unhappy following a review by the GP practice, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

Information Commissioner:

Wycliffe house
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745

<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 Practice Data Protection Officer.

If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as below.

Data Protection Officer:

The Practice Data Protection Officer is provided by SDS Myhealthcare. Any queries regarding Data Protection issues should be addressed to him at: -

Name: SDS MyHealthcare
Email: sdsmyhealthcare.ig@nhs.net
Postal: West Heath Medical Centre
194-196 West Heath Road
West Heath
Birmingham
B31 3HB

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 Practice Data Protection Officer.