

ANTICOAGULATION SERVICE PRIVACY NOTICE

Privacy Notice

How we Use Your Information in the Anticoagulation Service

About this notice

The purpose of this Notice is to tell you how we use your information to enable us to provide you with a Anticoagulation Service appointment.

What is the Anticoagulation Service?

The Anticoagulation Service provides you with a community-based safe and effective initiation, stabilisation, monitoring, dosing and prescribing 'One Stop Shop' oral anticoagulant management service. The service is provided out of 'Hubs' across Solihull.

Who we are and what we do

We, Solihealth Ltd (the Data Controller), are responsible for providing you with the Anticoagulation Service. We provide you with the ongoing care and support you may need from a qualified clinical team to manage your oral anticoagulation in the same way as your normal GP would.

The Anticoagulation Service is run by Registered Regulated GPs and is provided during surgery opening times.

Your information

The details below tell you what information we collect and hold about you, what we do with it, how we will look after it and who we might share it with. They also explain the choices you can make about the way your information is used and how you can opt out of any sharing arrangements that may be in place.

They cover information we collect directly from you or collect indirectly from other people or organisations who have provided services to you, such as hospitals, or other GPs.

This information is not exhaustive. We are happy to provide any additional information or explanation needed. Please see our contact details below:

Postal Address: [Solihealth Ltd
[179 Richmond Road, Olton, Solihull West Midlands B92
7SA]
Telephone Number: 0121 743 2159
E-mail Address: [Generic email address not yet available]

Caldicott Guardian

We have a person called a Caldicott Guardian who is responsible for making sure that your information is handled properly in line with your rights and the law. Our Caldicott Guardian is:

Caldicott Guardian: [Dr Anand Chitnis]
Contact Details: [0121 747 2422, c/o. The Castle Practice].

Senior Information Risk Owner

We have a Senior Information Risk Owner (known as a SIRO) who is responsible for ensuring that your information is handled securely. Our SIRO is:

Senior Information Risk Owner: [Mandy Holmes]
Contact Details: [0121 743 2159 ext 2068 – Solihealth Limited]

Data Protection Officer

We have a Data Protection Officer (known as a DPO) who is responsible for ensuring that your information is handled in accordance with our obligations under the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA18). Our DPO is:

Data Protection Officer: Paul Couldrey via PCDC Office]
Contact Details: [PCDC: 0115 838 6770].

How we use your information

We will use your personal information to enable us to book an appointment for you, to understand your medical history so that the anticoagulation GP/Nurse can provide you with high quality safe general medical care when you attend for your anticoagulation consultation. Your information will also be used to request tests and investigations and to refer you for treatment or further investigations.

Your information will also be used to design, develop, improve and pay for services funded by the NHS and to protect and improve the health of the public as a whole.

We make sure that any information we collect and use about you is protected and used in line with our duties under the General Data Protection Regulations (GDPR), the Data Protection Act 2018 (DPA18), the Human Rights Act 1998 and the Common Law Duty of Confidentiality.

We are registered as a Controller with the Information Commissioner's Office. A Controller is an organisation which is responsible for deciding how your information is handled and making sure that your information is protected and used appropriately. The Information Commissioner's Office is the organisation which makes sure that your information is handled properly.

Our Data Protection Registration Number is: [A8406960]. You can view our Data Protection Registration here: <https://ico.org.uk/ESDWebPages/Entry/Z5701332>].

How we make sure that your information is protected

Keeping your information safe and secure

We do a number of things to make sure that your information is safe, this includes making sure that the people we employ are honest and trustworthy and understand how they should handle your information safely.

We ensure that all laptops are encrypted, which means that any information held on them is scrambled so that someone who does not have the key cannot gain access to it.

We make sure that the computer systems we use are supported, secure and protected against people who should not have access to your information being able to see it.

Monitoring

We also carry out regular checks to make sure that the protection we have put in place is working properly and that your information is safe and secure.

External organisations

We also make sure that any organisations who provide services to us, or who we work with are honest and trustworthy and have the same sort of protection in place as we do, including making sure that the people they employ are fully trained and that checks have been made to make sure that they are trustworthy and honest before they are employed.

NHS staff duties

Everyone working for the NHS is required to comply with the General Data Protection Regulations, the Data Protection Act 2018, the Human Rights Act 1998 and the Common Law Duty of Confidence. Information provided to us in confidence will only be used for the purposes stated, unless there are other circumstances covered by the law.

Under the General Data Protection Regulations and the Data Protection Act 2018, all of our staff have to protect your information, inform you of how your information will be used, and let you decide if and how your information can be shared, unless we have a legal obligation, or a legitimate reason to do so. Any decisions you make about how we can use information we hold about you will be recorded along with that information.

Securely destroying your information when it is no longer needed

We only keep your information for as long as we need it to provide the service or comply with a legal obligation. When we no longer need to keep your information, we will securely destroy it.

If we have your information on paper, it will be stored in locked confidential waste bins until collected and securely shredded on-site by a commercial company]. Once your information is shredded, we receive a certificate to confirm that your information has been securely destroyed.

If we have your information on a computer system, all copies will be deleted when it is no longer required. Before any electronic storage devices are disposed of by Midlands and Lancashire CSU,

the device will either be physically destroyed, so that information cannot be retrieved from it, or the information will be overwritten multiple times, which results in the deleted information being completely removed from the device.

Information we may share

Sharing with other NHS organisations

Everyone working within the NHS has a legal duty to keep information about you confidential. Similarly, anyone who receives information from us has a legal duty to keep it confidential.

We will share information with the following main partner organisations:

- NHS Trusts and hospitals that are involved in your care
- Other General Practitioners where we refer you to another GP for a service that we do not provide
- Ambulance Services

We also share your information with NHS Digital who are legally allowed to collect information in identifiable form from us under Section 259(1) of the Health and Social Care Act 2012. You are able to opt out of this type of sharing by telling us that you do not wish to have your information shared in this way. For further information please see “Your right to opt out of sharing some types of information” below.

Sharing with non-NHS organisations

You may be receiving care from other organisations as well as the NHS, for example Social Care Services. We may need to share some information about you with them so we can all work together for your benefit if they have a genuine need for it or we have your permission.

Therefore, we may also share your information, subject to strict agreement about how it will be used, with:

- Social Care Services
- Education Services
- Local Authorities
- Voluntary and private sector providers working with the NHS

From time to time, there will new data sharing requirements as the NHS systems gradually work more closely together. For Birmingham and Solihull, this also covers our work around preventing emergency admissions to hospital which involves identifying patients at risk and discussing their medical history with teams from district and community nursing, social care and some voluntary sector organisations commissioned to provide support to these more vulnerable patients.

From time to time our services are subject to checking by organisation such as the Care Quality Commission and our local clinical commissioning group. They may look at your record to ensure we are keeping appropriate and accurate records and meeting NHS targets for quality and safety.

We will not disclose your information to any other third parties without your permission unless there are exceptional circumstances, such as if the health and safety of others is at risk or if the law requires us

to pass on information. If you choose not to agree to this when asked, we will record your decision to ensure that we do not share your information with that organisation in future.

If information is shared, we will only share the minimum amount of information necessary for them to provide the service or comply with their legal duty. We also ensure that an agreement is put in place which tells them what they can and can't do with your information and how they must protect it.

How long we keep your information

We only keep your information for as long as is necessary for the purpose we have collected it. We will keep information about your anticoagulation consultation and any information about tests and investigations requested, referrals made, medication prescribed and diagnoses made as a result of your anticoagulation consultation as part of your GP health record for a period of 10 years after death.

General information about how long NHS Organisations are required to keep different types of information can be found at: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care>

What to do if you are unhappy with the way we use your information

If you are concerned or not happy with the way we have collected or used your information, or you wish to raise a complaint, you can contact the Data Protection Officer, or alternatively the Practice Manager using the contact details above.

You can also tell the organisation which is responsible for making sure that your information is handled properly, this organisation is called the Information Commissioner's Office who can be contacted at:

Postal Address: Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow,
Cheshire
SK9 5AF

Telephone Number: 08456 30 60 60 or 01625 54 57 45

Website: www.ico.org.uk

Requesting access to your information

You are entitled to ask for a copy of the information held about you, or you can ask someone else to ask for a copy on your behalf.

A parent, guardian, a personal representative, or someone appointed by the Court can also request a copy.

How to request a copy of your records

If you want to obtain a copy of any records held about you, you will need to request this from your own GP Practice, as we only access your GP record for the purpose of the anticoagulation consultation. You will need to provide enough information to help your GP Practice find the records you are asking for. If you only want to request certain parts of your record, for example, records relating to a specific period of time, please tell them when you request your records. To make sure that they don't give your information to someone else, they will also need you to provide them with proof of your identity which needs to be:

- Current Passport and Photo Driving Licence and a bank or building society statement to prove your address.

If you are posting your original identification documents to your GP Practice, we would advise that you send them to us using Royal Mail Special Delivery, as this provides better protection, when sending identification documents, than the normal mail service, alternatively, you may hand deliver them. Once your GP Practice have confirmed your identity, they will return the documents to you using Royal Mail Special Delivery, which will require your signature.

Please send requests to your own GP Practice.

If you are unable to put your request in writing, or wish to make a verbal request, you will need to telephone your own GP Practice so that they can make alternative arrangements for you.

How much does it cost?

Under the General Data Protection Regulation organisations are not normally able to charge for the first copy of your record, however, if you request further copies, they are able to charge a fee based on our administrative costs for any additional copies.

How long will it take?

The law gives organisations up to one month from the date of receipt to provide you with the information you have requested, however, this period may be extended by a further two months where necessary, taking into account the complexity and number of requests. The response time is counted from the date enough information is received to help organisations to identify the records you have requested.

Withholding information about you

Organisations will not give you parts of your information which they believe could cause you, or someone else serious physical or mental harm. Organisations will not provide you with parts of your information which relate to someone else, unless they are a healthcare professional who has provided care to you.

Correcting inaccurate information

We have to ensure that your information is correct and up-to-date, it is important that you tell us about any changes, for example if you move house, or change your telephone number.

If you believe that any information held about you is wrong, is not complete, or is out of date, please contact us at the address below. If we agree that the information is wrong or not complete, we will put it right. If we do not agree that the information is wrong, we will make a note on your record that you believe that the information is wrong, not complete, or is out of date.

Further Information

If you have any queries or want to know more about the way we use your personal information, or if you don't want us to use your information in any of the ways listed below, please contact us using the details above.

The types of information we collect, use and share

Information which identifies you

The doctors, nurses and team of healthcare professionals caring for you, keep records about your health and any treatment and care you receive from the NHS. These records help to ensure that you receive the best possible care. They may be written down in paper records or held on computer. These records may include:

- Basic details about you such as name, address, date of birth, next of kin, landline and mobile telephone number etc, known as personal information and;

Sensitive personal information including:

- Contact we have had with you such as appointments or clinic visits.
- Notes and reports about your health, treatment and care.
- Results of x-rays, scans and laboratory tests.
- Relevant information from people who care for you and know you well such as health professionals and relatives.

It is essential that your details are accurate and up to date, especially telephone numbers. Always check that your personal details are correct when you visit us, contact us via our website or by telephone and please inform us of any changes as soon as possible. Landline and mobile telephone numbers may be used to provide appointment details via SMS text messages and automated calls to advise you of appointment times. As the messaging system develops we might also contact you by text regarding other matters concerning your health and care.

Information which does not identify you

Information may be used and shared for purposes other than direct care in forms which do not identify you, these include:

- **Anonymised** information – which does not tell us, or organisations we share it with, who you are
- **Pseudonymised** information - where your personal details have been changed to an alias, so that we don't know who you are (known as pseudonymised information).
- **Aggregated** information – which is information about many people, which is grouped into categories and only shows total numbers, or total financial values
- **Linked** information - some pseudonymised information we use and share is linked (using the alias) with other pseudonymised information about you.

Primary and secondary care information

There are two types of information which are collected and used to provide you with healthcare. The first is Primary Care Information; this is information which is collected and used when you visit us here at the Anticoagulation Service, the pharmacy, dentists and opticians for example. The second is Secondary Care information; this is information which is collected when you go to hospital for an outpatient appointment, x-rays or other tests, when you are admitted to hospital, if you go into a rehabilitation unit, or if you are admitted as an emergency to hospital for example.

Why we collect, use and share your information

We collect and use your information to provide you with direct healthcare services.

The doctors, nurses and team of healthcare professionals caring for you keep records about your health and any treatment and care you receive from the NHS. These records help to ensure that you receive the best possible care.

Information which identifies you is used to direct, manage and deliver the care you receive in an effective, efficient and safe way, to ensure that:

- The doctors, nurses and other healthcare professionals involved in your care have accurate and up to date information to assess your health and decide on the most appropriate care for you.
- Healthcare professionals have the information they need to be able to assess and improve the quality and type of care you receive.
- Your concerns can be properly investigated if a complaint is raised.
- Appropriate information is available if you see another doctor, or are referred to a specialist or another part of the NHS, Social Care or health provider

Information which would identify you

We will be using the following information to identify, treat and support you:

Your regular GP practice will make the first appointment for the Anticoagulation Service. In order to make an appointment, your GP Practice will need to provide us with enough information to enable us to make the appointment, this will include:

- Your NHS Number
- Your Name
- Your Address and Postcode
- Your Date of Birth
- Your Registered GP Practice Organisation Code

When you attend for your Anticoagulation service appointment we will ask you to complete a Registration Form which enables us to gather the following information about you, so that we can ensure that we can correctly identify you:

- Gender
- Forename and Surname
- Date of Birth
- NHS Number
- Home Address and Postcode
- Home Telephone Number
- Mobile Number
- Regular GP's Name
- GP Surgery Name
- Surgery Address

When you see the Anticoagulation Service GP / Nurse, the clinician will ask for your consent to directly access your GP health record. This will ensure that the GP treating you understands your medical history, so that he/she can ensure that any care given to you is safe and effective. The Anticoagulation Service GP / Nurse will be able to see the following information as part of your GP healthcare record:

- Contact your regular GP Practice or other organisations you have had with you, such as appointments or clinic visits.
- Notes and reports about your health, treatment and care.
- Results of x-rays, scans and laboratory tests.
- Relevant information from people who care for you and know you well such as health professionals and relatives.

The following restricted data items will also be included within your GP record:

- IVF, Fertility treatment and embryology;
- STIs;
- Gender realignment;
- HIV/AIDs diagnosis; and
- Termination of Pregnancy)

During the consultation, the Anticoagulation GP / Nurse will initiate, stabilise, monitor, dose and prescribe an anticoagulant. The GP / Nurse will ask you for , other information which may support your consultation. . This information, along with the information included in your medical history and INRstar record will help the GP to provide you with the care you need.

The Anticoagulation GP / Nurse will directly update your record during the consultation. A copy of this information will also be transferred to your GP healthcare record

Legal basis for collection

The legal basis for us to collect and use your information for this purpose is:

Article 6(1)(e) "...for the performance of a task carried out in the public interest or in the exercise of official authority..."

and

Article 9(2)(h) "...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems..."

How long we keep your information

We will keep information collected and used as part of the Anticoagulation Service, stored within your GP health record for 10 years after death.

Organisations we share your information with

We will share your information when referring you to organisations who are working with us to provide direct care to you, for example hospitals, community service providers, social care, voluntary organisations, private organisations. In all circumstances we will provide partner organisations with the minimum information to enable them to identify you and to understand the reason for referral.

When we have referred you to another care provider for tests, investigations or treatment, in most cases, your GP is provided with information about your visit, to ensure that they know about any new diagnoses, any drugs you may have been prescribed and any treatments you may have received. This ensures that any ongoing care they provide to you does not conflict with the care provided by the other healthcare provider and enables your GP to complement and support that care.

Your data protection rights

If you wish to exercise any of your rights please use the contact details below:

Postal Address: – FAO Practice Manager
Bosworth Medical Centre, Chelmsley Wood Primary Care Centre,
Crabtree Drive, Chelmsley Wood, B37 5BU
0121 770 4484

The right to object to processing

Where the legal basis we are relying upon is Article 6(1)(e), as above, you have the right to object to the processing of your personal data for this purpose. If you choose to object to processing for this purpose, we cannot process your personal data any further, unless we can demonstrate compelling grounds for the processing which override your right to object, or where we need to process your personal data for the establishment, exercise, or defence of legal claims. If you wish to object to the processing or sharing of your personal information, we will discuss this with you so that you understand how your decision to object may affect the care we are able to provide to you.

As your information is stored on your usual GP Practice's system, any objection should be made to your usual GP Practice.

The right to restrict processing

You have a right to restrict processing of your personal information in situations where:

- you are contesting the accuracy of your data and aware awaiting the organisation holding your data to verify it;
- the processing of your data has been identified as unlawful, but you do not want the organisation holding your data to delete it;
- if we no longer need to keep your information, but you want it to be retained in order that you can establish, exercise or defend a legal claim
- you have objected to the processing and the organisation holding your data are in the process of determining whether our legitimate grounds for processing override your interests, rights and freedoms.

As your information is stored on your usual GP Practice's system, any request to restrict processing should be made to your usual GP Practice.

The right to erasure

You have a right to have all of your data deleted from systems upon which it is held, where you have objected to processing and the organisation holding your data have not been able to demonstrate that our legitimate grounds for processing override your interests, rights and freedoms. When reviewing your request, we will take into consideration that your medical information has been collected and stored by us to ensure that we can continue to provide you with safe and effective care, and also for the purpose of establishing, exercising, or defending legal claims.

As your information is stored on your usual GP Practice's system, any request to erase your data should be made to your usual GP Practice.

The right to rectification

You have a right to ask organisations holding your data to rectify any inaccurate data, make incomplete data incomplete and to request that you make a supplementary statement to attach to your record.

As your information is stored on your usual GP Practice's system, any request to rectify the data held should be made to your usual GP Practice.

Your right to opt out of sharing some types of information

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

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

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

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

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

You have a choice about whether you want your confidential patient information to be used in this way.

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

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters.

On this web page you will:

- See what is meant by confidential patient information

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

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

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research); and <https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made).

You can change your mind about your choice at any time.

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

Health and care organisations have until 2020 to put systems and processes in place so they can apply your national data opt-out choice. Our organisation is not currently able to apply your national data opt-out choice to any confidential patient information we may use or share with other organisations for purposes beyond your individual care.

Letting you know when things change

We check these details regularly to make sure that they are up to date and tell you how we are using your information. The last time these details were checked was June 2018.