

SPRINGFIELD SURGERY

Springfield Way, Brackley, Northants, NN13 6JJ

Privacy Notice

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 that we may collect from or about you.

This privacy notice applies to personal information processed by or on behalf of the practice.

This Notice explains

- Who we are, how we use your information and our Data Protection Officer
- What kinds of personal information about you do we process?
- What are 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 by us?
- What are your rights under data protection laws?

The General Data Protection Regulation (GDPR) became law on 24th May 2016. This is a single EU-wide regulation on the protection of confidential and sensitive information. It enters into force in the UK on the 25th May 2018, repealing the 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 (currently in Bill format before Parliament) the practice responsible for your personal data is Springfield Surgery.

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

Springfield Surgery will be what's known as the 'Controller' of the personal data you provide to us.

We collect basic personal data about you which does not include any special types of information or location-based information. This does however include name, address, 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 gender during the services we provide to you and or linked to your healthcare through 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 (e.g. 111, NHS Trust, GP Surgery, Walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

NHS health records may be electronic, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Records which the Practice hold about you may include the following information;

- Details about you, such as your address, carer, legal representative, emergency contact details
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments, etc.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests, x-rays etc
- Relevant information from other health professionals, relatives or those who care for you

To ensure you receive the best possible care, your records are used to facilitate the care you receive. Information held about you may be used to help protect the health of the public and to help us manage the NHS. Information may be used within the GP practice for clinical audit to monitor the quality of the service provided.

How do we lawfully use your data?

We need to know 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 particular condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention.

Information about you is collected from a number of sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information using software and is only 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.

Medicine 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. This service is provided to practices within Nene Clinical Commissioning Group.

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 and General Data Protection Regulation 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 new 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. They should be supported by the policies of their employers, regulators and professional bodies.

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

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 Springfield Surgery an appropriate contract (part 24-28) will be established for the processing of your information.

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

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

We would however like to use your name, contact details and email address to inform you of services that may benefit you, with your consent only. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends.

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.

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. 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.

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
- 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 Digital
- 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 explicit consent for this happen when this is required.

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 Springfield Surgery an appropriate contract (art 24-28) will be established for the processing of your information.

Who are our partner software suppliers/businesses?

We use a number of different pieces of software and organisations outside of the NHS to facilitate your healthcare and to enable our staff to contact you. These are as follows:

Company Name	Description of Service	Can employees of the organisation access patient information?	Location of GDPR Statement
EMIS	Clinical system which holds patient demographic and medical information – remote server	The servers and the connection to the practice are encrypted, so EMIS staff are not able to access patient information in this way. However EMIS support staff are able to dial in remotely with the consent of our staff for problem solving.	https://supportcentre.emishealth.com/emis-group-and-the-gdpr-general-data-protection-regulation/
Connect2/A CR Networks	Telephone system – call recording onto a server located within the practice	All recordings are physically located on the server within the practice. All support and problem solving would be done by a representative of the company attending the practice. They do not have the ability to dial in remotely.	http://www.connect2tele.com/gdpr-information/
MJog	SMS and smart messaging system between the practice and the patients	Patient's EMIS (clinical system) numbers are uploaded to MJog website. The website has an encrypted link to the patient database which is interrogated for the patient's name and mobile number. MJog employees would only have access to this identifiable information when troubleshooting – they will sometimes dial in to an HEMC staff member's PC with the consent of the member of staff to fix a problem.	https://www.mjog.com/privacy-policy/ https://www.mjog.com/gdpr-approaches-new-data-protection-legislation/ https://www.mjog.com/data-protection-changes-weeks-away/
Docman	Clinical software which holds patient letters and documents	Docman support staff can remotely dial in with the consent of our staff for problem solving.	https://www.docman.com/privacy-policy/
Docmail	External printing and mailing agency who we use to send large batches of letters	Docmail staff can dial in remotely with the consent of our staff for problem solving.	http://www.cfhdocmail.com/tob.html
Shredit	Shred paper which has patient data or other confidential data	Representative comes to site and collects the 3 shredding bins and shreds on site.	https://www.stericycle.com/Stericycle/GDPR/PrivacyPolicy/PrivacyNotice_EN.html
Crescendo (Including Dragon)	Dictation software which clinical staff use to dictated	Support staff can dial in remotely with the consent of our staff for problem solving.	http://crescendosystems.co.uk/privacypolicy.html

Voice Recognition Software)	letters for secretaries to type		
Numed	Numed provide software and support for our ECG machine	Support staff can dial in remotely with the consent of our staff for problem solving.	https://www.numed.co.uk/gdpr-statement-of-compliance
Welch Allyn	Provide software and support for Ambulatory BP Machine	Support staff can dial in remotely with the consent of our staff for problem solving.	https://www.welchallyn.com/en/other/privacy-policy.html
NELCSU	Provide IT support for the practice	Support staff can dial in remotely or attend the practice in person for problem solving and software updates.	Kept in file in Practice Manager's office
PML	Providing summarising of new patient medical records onto EMIS (clinical system)	Employee of PML comes into the surgery. No medical information is taken off site.	https://www.principal-medical.co.uk/privacy-policy/
SDS Storage	Secure storage facility for medical records	Storage facility who hold all paper records for patients. Employees of SDS courier medical records securely between the practice and the storage facility. Online catalogue of records held is encrypted.	https://www.shredall.co.uk/privacy-policy
Accurx	Text messaging and video calling software	Yes, all data is encrypted.	https://www accurx.com/gdpr-questions

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 because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply.

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 market to you, you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will Delete your data but will generally assume that you would prefer us to keep a note of your name on our register of individuals who would prefer not to be contacted. That way, we will minimise the chances of you being contacted 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

Access to personal information / Subject Access Requests

Data Subject Access Request (DSAR): You have a right under the General Data Protection Regulations 2018 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. In order to request this, you need to do the following:

- You must complete an 'Access to Health Records' form which is available from reception.
- You will be offered three different ways of accessing your records (a leaflet will be provided to you with the 'Access to Health Records' form): online access, electronic record only access or full copy of records including paper records. There may be a charge to have a full printed copy of your records if the administrative burden of photocopying and printing is deemed as excessive.
- Once the level of access has been agreed this access will be provided within month. If you are collecting paper copies of the records from reception you will be required to bring photographic ID when you come to collect. Records cannot be collected by someone else on your behalf.

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 Practice Manager - Hayley Willingham, email address: Hayley.Willingham1@nhs.net) by email, telephone or letter or contact our Data Protection Officer as below. If you are still unhappy following a review by the GP practice, you can then complain to the Information Commissioners Office (ICO):

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 extracted and 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 Paul Couldrey of PCIG Consulting Limited. Any queries in regard to Data Protection issues should be addressed to him at: -

Email: Couldrey@me.com
Postal: PCIG Consulting Limited
7 Westacre Drive
Quarry Bank
Dudley
West Midlands
DY5 2EE

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 – contact details as above.