Privacy Notice

1. INTRODUCTION

This Privacy Notice provides you with details of how we collect and process your personal data within St Thomas Medical Group, including any information you may provide through our website, in person or via our registration form. By providing us with your data, you confirm to us that you are over 13 years of age.

St Thomas Medical Group is the data controller and we are responsible for your personal data. We are registered with the Information Commissioners Office as a Data Controller and our registration number is Z6659160.

If you have any questions about this privacy notice, please contact the Data Protection Officer using the details set out below.

Contact Details

Full name of Data Controller: **St Thomas Medical Group**

Name of Data Protection Officer: **Nina Smith**

Email address: **d-ccg.stthomasm@nhs.net**

Postal address: **St Thomas Health Centre, Cowick Street, St Thomas, Exeter, EX4 1HJ**

If you are not happy with any aspect of how we collect and use your data, you have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (*www.ico.org.uk*). We should be grateful if you would contact us first if you do have a complaint so that we can try to resolve it for you.

It is very important that the information we hold about you is accurate and up to date. Please let us know if at any time your personal information changes by emailing us at Stthomas@nhs.net OR by attending the surgery and completing our change of details form.

2. WHAT DATA DO WE COLLECT ABOUT YOU?

Personal data means any information capable of identifying an individual. It does not include anonymised data.

We may process certain types of personal data (including Special Category Data) about you as follows:

- Details about you, such as your name, address, carers, biological gender, gender identity, ethnic origins, date of birth, legal representatives and 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.

3. HOW IS MY DATA STORED?

Our practice uses a clinical records programme called EMIS Web, which is where electronic information about you will be stored. EMIS Health Ltd act as the data processor for this. Any information held in paper records is stored securely at the Practice. We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

4. 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.
- Payment providers (if for example you were paying for a service such as travel vaccinations)

When a new provider/service is selected, a Data Protection Impact Assessment is carried out to ensure compliance and safety of your personal data. These are available on request.

5. WHAT IS THE LEGAL BASIS THAT WE USE TO PROCESS YOUR INFORMATION?

Generally, we do not rely on consent as a legal ground for processing your personal data, other than in relation to sending marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by emailing us at **Stthomas@nhs.net**

Purposes for processing your personal data
Set out below is a description of the ways we intend to use your personal data and the legal basis on which we will process such data. We have also explained what our legitimate interests are where relevant.

We may process your personal data for more than one lawful ground, depending on the specific purpose for which we are using your data.

Purpose/Activity	**Legal basis for processing under the UKGDPR**	**Special category of data under the UKGDPR**
Provision of direct care and related administrative purposes. e.g. Referrals to hospitals or other care providers	Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	Article 9 (2)(h) – processing is necessary for the purposes of preventive or occupational medicine, 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 on the basis of Union or Member State law or pursuant to contract with a health professional.
For commissioning and healthcare planning purposes. e.g. Collection of mental health data set via NHS digital or local.	Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.	Article 9 (2)(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 and services on the basis of Union or Member State law or pursuant to contract with a health professional. UKGDPR Article 9 (2)(i) – processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high

		standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
For planning and running the NHS (other mandatory flow) e.g. CQC powers to require information and records	Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	UKGDPR Article 9 (2)(h) – medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems. UKGDPR Article 9 (2)(i) – public interest in the area of public health.
For planning & running the NHS – National Clinical Audits	Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	UKGDPR Article 9 (2)(h) – medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems. UKGDPR Article 9 (2)(i) – public interest in the area of public health.
For research * *You can opt-out of your data being used for research by visiting – www.nhs.uk/your-nhs-data-matters	Article 6 (1)(a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 6 (1)(f) – processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal, in particular where the data subject is a child.	UKGDPR Article 9 (2)(j) – scientific or historical research purposes or statistical purposes.
For safeguarding or other legal duties	Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject. Article 6 (1)(d) – processing is necessary in order to protect the vital interests of the data subject or of another natural person. Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	UKGDPR Article 9 (2)(b) – purposes of carrying out the obligations of social protection law.
During an epidemic - For understanding risks to public health, controlling and preventing spread, identifying	Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.	UKGDPR Article 9 (2)(h) – medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems.

and informing at risk patients and trends	Article 6 (1)(d) – processing is necessary in order to protect the vital interests of the data subject or of another natural person. Article 6 (1)(e) – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	UKGDPR Article 9 (2)(i) – public interest in the area of public health.
When you ask us to share your information e.g. subject access requests or we are ordered by a Court to provide records	Article 6 (1)(a) – the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Article 6 (1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.	UKGDPR Article 9 (2)(a) – explicit consent. UKGDPR Article 9 (2)(c) – processing is necessary to protect the vital interests of the data subject

6. HOW LONG DOES THE PRACTICE HOLD MY INFORMATION?

As long as you are registered as a patient with **St Thomas Medical Group**, your paper records are held at the practice along with your GP electronic record. If you register with a new practice, they will initiate the process to transfer your records. The electronic record is transferred to the new practice across a secure NHS data-sharing network and all practices aim to process such transfers within a maximum of 8 working days. The paper records are then transferred via Primary Care Services England (operated on behalf of NHS England by Capita) which can take longer. Primary Care Services England also looks after the records of any patient not currently registered and the records of deceased patients.

Once your records have been forwarded to your new practice (or after your death forwarded to Primary Care Services England), a cached version of your electronic record is retained in the practice and classified as "inactive". If anyone has a reason to access an inactive record, they are required to formally record that reason and this action is audited regularly to ensure that all access to inactive records is valid and appropriate. We may access this for clinical audits (measuring performance), serious incident reviews, or statutory report completion (e.g. for HM Coroner)

7. RIGHT OF CORRECTION, ERASURE AND RESTRICTION

It is your duty to inform us of changes
It is important that you tell the person treating you if any of your details, such as your name or address have changed or if any of your details such as date of birth are incorrect, so that this can be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

Your rights in connection with personal information
Under certain circumstances, by law you have the right to request:

- **Rectification**: to ask us to change any personal data which is wrong
  If you think the data we hold on you is inaccurate or incomplete, you may ask us to rectify or complete it.
- **Erasure:** to ask us to delete any personal data we hold. This is sometimes referred to as 'the right to be forgotten'.
  Under the UKGDPR you sometimes have the right to have personal data erased, however, this does not apply to many of our key data holdings such as health records as we are keeping such records as part of our legal duties.
- **Restriction:** to ask us not to process your information for certain purposes. There is also a specific right to ask us not to use your contact details for marketing purposes.
  This is closely linked to other rights. You have the right to restrict processing in limited circumstances, for example if you think our data is inaccurate and you want to limit what we do with it until we have considered rectification.

- **Objection:** to object to some types of processing based on your own individual circumstances.
  You have a general right to object to our processing your personal data if we are processing your information for direct marketing. We will always respect such an objection.
- **Data portability:** to receive your information in a specific form so that it can be used by another organisation. However, this right only applied where we are processing information by consent, so it does not apply to medical records.

You can make a request by contacting our Data Protection Officer by post or email. We will tell you within one month what action we intend to take in response to your request.

For more information, please see the Information Commissioner's website.

8. HOW CAN I SEE WHAT INFORMATION YOU HOLD ABOUT ME?

You have a right under data protection legislation to request to see what information the practice holds about you. You also have the right to ask for inaccuracies to be corrected and in some circumstances you have the right to request that we stop processing your data. Some of these rights are not automatic and we reserve the right to discuss with you why we might not comply with a request from you to exercise them.

If you make a Subject Access Request (SAR), we will:

- Describe the information we hold about you.
- Tell you why we are holding that information.
- Tell you who it might be shared with.
- At your request, provide a copy of the information in an easy to read form.

In order to request this, you need to do the following:

- Your request must be made in writing (a form can be collected from the surgery, emailed to you or downloaded from https://www.stthomasmedicalgroup.co.uk/practice/access-to-medical-records/
- We will provide printed or electronic copies (by online access, by email or if you wish you can bring in a USB memory stick)
- We are required to respond to your request within 1 month.
- We ask that you show provide valid ID before the copies can be provided to you.

You will need to give as much information as you can so that your identity can be verified and your records located.

In some circumstances (where the request is unfounded, repeated or excessive), there may be a charge to have a printed copy of the information held about you. If this is the case, this will be discussed with you before any charge is made.

9. HOW IS MY INFORMATION USED?

For the provision of direct care:
In the practice, individual staff will only look at what they need in order to carry out tasks such as booking appointments, making referrals, giving health advice or to provide you with care.

Sometimes your information may be used to run automatic calculations. These can be as simple as calculating your Body Mass Index, but they can be more complex and used to calculate some risks to your health that we should consider with you. The ones we use at St Thomas Medical Group include Qrisk (cardiovascular risk assessment – usually following a NHS Healthcheck), Qdiabetes, GP2DRS and eFI (electronic frailty index). Whenever we use these profiling tools, we assess the outcome on a case-by-case basis. No decisions about individual care are made solely on the outcomes of these tools, but they are used to help us assess and discuss your possible future health and care needs with you.

We share information about you with other health care professionals/services, where they have a genuine need for it or to support your care, as follows.

Royal Devon & Exeter NHS Foundation Trust	Secondary or Emergency Care
Devon Partnership Trust	Secondary or Emergency Care
Other national providers of health care who you choose to be referred to, in consultation with your health care professional	Secondary or Specialist Care
NHS National Diabetes Prevention Programme	Information and lifestyle education
NHS Screening Programmes	Information and Specialist Care
SW CHIS (Child Health Information Service) www.swchis.co.uk (privacy notice)	Healthy Child Programme & Childhood Vaccinations
Devon Doctors/111	Out of hours Primary Care
Exeter City Council	Social Care Services
PRIMIS (University of Nottingham)	NHS Partner
UK Biobank	Data extract of anonymised data for research purposes (only where patients have registered with UK Biobank and provided their explicit consent)
Hospiscare	Specialist Care – Hospiscare will have access to 'view' certain parts of your medical record for the provision of care, but only whilst you are under their service.
GP Connect	Allows GP practices and authorised clinical staff to share and view GP practice clinical information and data e.g. if you are elsewhere in the country and need medical treatment, a clinician can view your medical record with your consent. This will initially allow 111 to book appointments directly with the surgery.
Pinnacle/Outcomes4Health	Outcomes4Health is a web-based system which has been approved by NHS England for the management of the COVID-19 vaccination programme.
NHS Digital and Oxford University (COVID-19 Risk Assessment Tool)	GP Practices have the option of using the COVID-19 Risk Assessment Tool to help identify patients more at risk of coronavirus and it's complications. No patient identifiable information is input or stored within the Tool and the use of the Tool would be discussed with you prior to use.

For commissioning and healthcare planning purposes:
In some cases, for example when looking at population healthcare needs, some of your data may be shared (usually in such a way that you cannot be identified from it). The following organisations may use data in this way to inform policy or make decisions about general provision of healthcare, either locally or nationally.

- Exeter City Council: Public Health, Adult or Child Social Care Services.
- Northern, Eastern and Western Devon Clinical Commissioning Group
- NHS Digital
- UK Government (Department of Health & Social Care)
- Other data processors which you will be informed of as appropriate.

In order to comply with its legal obligations, we may send data to NHS Digital when directed by the Secretary of State for Health and Social Care under the Health and Social Care Act 2012.

The practice contributes to national clinical audits and will send the data which is required by NHS Digital, when the law allows. This may include demographic data, such as date of birth, and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.

For research purposes:
Research data is usually shared in a way that individual patients are non-identifiable. Occasionally where

research requires identifiable information, you may be asked for your explicit consent to participate in specific research projects. The surgery will always gain your consent before releasing any information for this purpose.

Where specific information is asked for, such as under the National Diabetes Audit, you have the choice to opt out of the audit.

For safeguarding purposes, life or death situations or other circumstances where we are required to share information:
We may also disclose your information to others in exceptional circumstances (i.e. life or death situations) or in accordance with Dame Fiona Caldicott's information sharing review (information to share or not to share)

For example, your information may be shared in the following circumstances:

- When we have a duty to others e.g. in child protection cases.
- Where we are required by law to share certain information such as the birth of a new baby, infectious diseases that may put you or others at risk or where a Court has decided that we must.

For invoice validation:
If you have received treatment within the NHS, the CCG may require access to your personal information in order to determine which Clinical Commissioning Group should pay for the treatment or procedure you have received.

Information such as your name, address and date of treatment may be passed on to enable the billing process. These details are held in a secure environment and kept confidential. This information will only be used to validate invoices, and will not be shared for any further Commissioning purposes.

When you request to see your information or ask us to share it with someone else:
If you ask us to share your data, often with an insurance company, solicitor, employer or similar third party, we will only do so with your explicit consent. Usually the requesting organisation will ask you to confirm your consent, often in writing or electronically. We check that consent before releasing any data or you can choose to see the information before we send it.

Further Information

Further information about the way in which the NHS uses personal information and your rights in that respect can be found in:

The NHS Care Record Guarantee: http://www.nigb.nhs.uk/pubs/nhscrg.pdf

The NHS Constitution: https://www.gov.uk/government/publications/the-nhs-constitution-for-england

The HSCIC Guide to Confidentiality gives you more information on the rules around information sharing: http://content.digital.nhs.uk/media/12822/guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf

An independent review of how information about patients is shared across the health and care system was conducted in 2012 by Dame Fiona Caldicott. The report, Information: To share or not to share? The Information Governance Review, can be found at: https://www.gov.uk/government/publications/the-information-governance-review

NHS England – Data Services for Commissioners provides further information about the data flowing within the NHS to support commissioning: https://www.england.nhs.uk/ourwork/tsd/data-services/

Please visit NHS Digital's website for further information about their work. Information about their responsibility for collecting data from across the health and social care system can be found at: https://digital.nhs.uk/about-nhs-digital/our-work

The Information Commissioners Office is the Regulator for the Data Protection Act 2018 and offer independent advice and guidance on the law and personal data, including your rights and how to access your personal information. For further information please visit the Information Commissioners Office website at https://ico.org.uk