

Total Health Excellence East & West (THEEW) Primary Care Networks

Data Protection Privacy Notice

As THEEW Primary Care Network (Aylesham Medical Practice, Lydden Surgery, Pencester Surgery, Whitecliffs Medical Centre, The New Surgery, Manor Clinic, Sandgate Road Surgery and Guildhall Street Surgery), we understand how important it is to keep your personal information safe and secure, and we take this very seriously. We have taken steps to make sure your personal information is looked after in the best possible way, and we review this regularly. We have robust policies and procedures in place including an Information Governance Policy. We have also adopted a 'privacy by design' approach and this helps to ensure that we consider the privacy implications of our systems and services.

Please read this Privacy Notice carefully as it contains important information about how we use your personal and healthcare information that you give to us, or any information that we may collect from you or about you from other organisations.

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)

For how long your personal information is retained/stored

What are your rights under Data Protection laws

The Categories of Personal Information

Dependent on the purpose of processing, different categories of data may be used by the Practice. Data can be categorised using the following terms:

Anonymised data – data where personal identifiable identifiers have been removed. Data protection laws and the Common Law of Confidentiality do not apply to anonymised data.

Pseudonymised data – data where any information which could be used to identify an individual has been replaced with a fake identifier. Pseudonymised data remains personal data and as such the Common Law Duty of Confidentiality and Data Protection legislation apply and there must be a lawful reason for using such data.

Person identifiable information (or personal data) – any information about an individual from which, either on its own or together with other information, that person may be identified. The Common Law Duty of Confidentiality and Data Protection legislation apply and there must be a lawful reason for using such data.

To find out more about the data processed for each purpose, please click on the links below (The Purpose(s) of Processing).

In addition to the above types of data, some information is considered protected regardless of the purpose of processing; this information does not form part of your shared care record and is not disclosed 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 such information.

The Purpose(s) of Processing Personal Data

Your Practice will process data for the following purposes:

- Direct Care
- Human Resources
- Research
- Statutory Purposes
- [Kent and Medway Care Record Privacy Notices](#)

Legal Justification for Collecting and using your Information

The law says we need a legal basis to handle your personal and healthcare information.

Contract: We have a contract with NHS England to deliver healthcare services to you. This contract provides that we are under a legal obligation to ensure that we deliver medical and healthcare services to the public.

Consent: Sometimes we also rely on the fact that you give us consent to use your personal and healthcare information so that we can take care of your healthcare needs.

Please note that you have the right to withdraw consent at any time if you no longer wish to receive services from us.

Necessary care: Providing you with the appropriate healthcare, where necessary. The Law refers to this as 'protecting your vital interests' where you may be in a position not to be able to consent.

Law: Sometimes the law obliges us to provide your information to an organisation (see above).

Special Categories

The law states that personal information about your health falls into a special category of information because it is sensitive. Reasons that may entitle us to use and process your information may be as follows:

Public Interest: Where we may need to handle your personal information when it is considered to be in the public interest. For example, when there is an outbreak of a specific disease and we need to contact you for treatment, or we need to pass your information to relevant organisations to ensure you receive advice and/or treatment

Consent: When you have given us consent

Vital Interest: If you are incapable of giving consent, and we must use your information to protect your vital interests (eg if you have had an accident and you need emergency treatment)

Defending a claim: If we need your information to defend a legal claim against us by you, or by another party

Providing you with medical care: Where we need your information to provide you with medical and healthcare services

Organisations We Share your Personal Information with

Personal Data (including special category data) will only be shared between the general Practice and health and social care organisations that have signed a Joint Controller or Data Processing Agreement. Whenever you use a health or care service, such as attending Accident and Emergency or using Community Care Services, important information about you is collected to help ensure you get the best possible care and treatment. This information may be passed to other approved organisations where there is a legal basis, to help with planning services, improving care, research into developing new treatments and preventing illness. All of this helps in providing better care to you and your family and future generations. However, as explained in this Privacy Notice, confidential information about your health and care is only used in this way as allowed by law and would never be used for any other purpose without your clear and explicit consent.

We may pass your personal information on to the following people or organisation because these organisations may require your information to assist them in the provision of your direct healthcare needs. It, therefore, may be important for them to be able to access your information to ensure they may professionally deliver their services to you. These currently include:

- Dartford and Gravesham NHS Trust (D&G)
- East Kent Hospitals University NHS Foundation Trust (EKHUFT)
- Medway Maritime Hospital - Medway NHS Foundation Trust (MFT)
- Maidstone and Tunbridge Wells NHS Trust (MTW)
- Kent and Medway Partnership NHS and Social Care Partnership Trust (KMPT)
- North East London Foundation Trust (NELFT)
- Kent Community Health NHS Foundation Trust (KCHFT)
- HCRG Care Group Limited
- Pilgrims Hospices
- South East Coast Ambulance Service (SECAmb)
- Integrated Care 24 (IC24)
- Out of hours providers (currently IC24, SECAmb, KCC Children's Services)
- NHS Kent and Medway
- Kent County Council (children and adults social care departments) (KCC)
- Medway Council (children and adults social care departments) (MWC)
- GP federations.

- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Health care partnerships
- Other Kent & Medway Primary Care networks that we work in partnership with
- Mental Health providers
- Community trusts
- Kent County Council/Medway council Social Care Services
- NHS England
- Police & Judicial Services

Multi-Disciplinary Team Meetings

Sharing of personal and special category information is for direct patient care, to enable people to receive care at the right place and the right time, for the best value. Purpose of the sharing includes:

- Providing a centrally coordinated response for people and residents of Total Health Excellence East and West PCN's who need to access Health and Wellbeing services.
- Enabling people to tell their story once with the aim of improving better service delivery.
- Enabling professionals to access information they needed, when they needed it, to support better outcomes for local people
- Enabling professionals to work together to support a person's need and ensure the right level of support is given
- Reducing hospital admissions by providing early support and avoid an escalation of needs

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 organisation. 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 your registered practice for further information about opt out.

Individual Risk Management at a GP practice level however is deemed to be part of

Kent and Medway Shared Care Record

Patients in Kent and Medway can benefit from the sharing of information to better manage their care via the Shared Care Record system. This includes sharing: contact details, diagnosis, medications, allergies, test results, referral and letters and care plans between health professionals

Being able to see this information will help them give you the best care as quickly as possible without having to make phone calls or wait for other organisations to forward details on. Some of their administrative and secretarial staff will also be able to see information so they can support the professionals. An example would be to send you an appointment letter.

All staff must follow the law on keeping your information confidential. Each time they look at your records this will be recorded to make sure they are only looking at the right information, for the right reasons.

Summary Care Records

Your Summary Care Record (SCR) is an electronic record of important patient information created from the GP medical records. It contains information about medications, allergies and any bad reactions to medications in the past. It can be seen by staff in other areas of the health and care system involved in your direct care.

During the height of the pandemic, changes were made to the SCR to make additional patient information available to all appropriate clinicians when and where they need it, to support direct patient care, leading to improves 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 SCR preferences, you will still have the same options that you currently have in place to opt out of having a SCR including the opportunity to opt back in to have a SCR or opt back in to allow sharing of additional information. Further details about the SCR and your choices can be found here - [Summary Care Record supplementary transparency notice - NHS England Digital](#)

NHS Digital Data Collection from THEEW PCN

The NHS needs data about the patients it treats to plan and deliver its services and to ensure that care and treatment provided is safe and effective. The General Practice Data for Planning and Research data collection will help the NHS to improve health and care services for everyone by collecting patient data that can be used to do this.

For example, patient data can help the NHS to:

- monitor the long-term safety and effectiveness of care
- plan how to deliver better health and care services
- prevent the spread of infectious diseases
- identify new treatments and medicines through health research

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

The PCN contributes to national clinical audits and will send the data, which is required by NHS England 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.

To find out more or to register your choice to opt out, please visit Your NHS Data Matters. [We need to check who you are before you can make your choice - NHS National Data Opt-Out Service](#)

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

Service Evaluation

The PCN carries out service evaluations to improve the quality and accessibility of primary care services. This may be carried out in several ways including telephone surveys, online surveys and interviews.

The legal basis for contacting you to take part -

- *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*

To process the survey information we collect from you, we will only do so with your consent.

- *Article 6(1)(a) - Consent of the data subject (you)*
- *Article 9(2)(a) – Explicit consent of the data subject. (you)*

Population Health Management

Population Health Management (or PHM for short) is aimed at improving the health of an entire population. It is being implemented across the NHS and the PCN is taking part.

PHM is about improving the physical and mental health outcomes and wellbeing of people and making sure that access to services is fair, timely and equal. It helps to reduce the occurrence of ill-health and looks at all the wider factors that affect health and care.

The PHM approach requires health care organisations to work together with communities and partner agencies, for example, GP practices, community service providers, hospitals and other health and social care providers.

These organisations will share and combine information with each other in order to get a view of health and services for the population in a particular area. This information sharing is subject to robust security arrangements.

How will your Personal Data be used

Information about your health care, which includes personal data, will be combined to create a picture of your health care.

Anything that can identify you will be removed and will be replaced with a unique code, so that people working on that data will only see the code and cannot see any personal data.

This means that the people working with the data will only see the code and cannot see which patient the information relates to.

If we see that an individual might benefit from some additional care or support, we will send the information back to your GP or hospital provider and they will use the code to identify you and offer you relevant services.

Examples of how the information could be used for several healthcare related activities include:

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

Is using your Personal Data in this way Lawful

Health and Social Care Providers are permitted by data protection law to use personal information where it is 'necessary for medical purposes. This includes caring for you directly, as well as management of health services more generally.

Some of the work that happens at a national level with your pseudonymised personal information is enabled by other legislation. Sharing and using your information in this way helps 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, and, unless directly for your care, pseudonymised data is used so that you cannot be identified.

Can you Object to your Personal Data being used as part of Population Health Management

You have a right to object to your personal information being used in this way. If you do choose to 'opt out' please contact the practice. If you are happy for your personal information to be used as part of this project then you do not need to do anything further, although you do have the right to change your mind at any time.

If you still have concerns, you can also contact the Information Commissioner's Office directly via their helpline on 0303 123 1113.

Who is the Data Controller

Your registered practice is the Data Controller of your personal data under the Data Protection Act 2018. We will collect basic personal data about you and location-based information. This means we are responsible for collecting, storing and handling your personal and healthcare information when you are seen by us as a patient.

There may be times when we also process your information. That means we use it for a particular purpose and, therefore, on those occasions we may also be data processors.

Information We May Collect From You

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 held by this organisation may include the following information:

- Your contact details (such as your name, address and email address including place of work and work contact details)
- Details and contact numbers of your next of kin
- Your age range, gender, ethnicity
- Details in relation to your medical history
- The reason for your visit
- Any contact the PCN has had with you, including appointments (emergency or scheduled), clinic visits, etc.

- Notes and reports about your health, details of diagnosis and consultations with our GPs and other Health Professionals within the healthcare environment involved in your direct healthcare
- Details about treatment and care received
- 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, 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 PCN practices for clinical audit to monitor the quality of the service we provided.

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.

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. These secure transfers will be backed by appropriate data processing agreements.
- No third 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.

- The PCN operates a clinical computer system called EMIS 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.
- From 10th June 2019, EMIS, as data processor, started storing this organisation's EMIS Web data in a highly secure, third-party cloud hosted environment, namely Amazon Web Services ("AWS").
- This data will always remain in the UK 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 organisations.

Third Party Processors

To deliver the best possible service, the PCN will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the PCN 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 websites 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.

Anonymised Information

Sometimes we may provide information about you in an anonymised form. Such information is used to analyse population-level health issues and helps the NHS to plan better services. If we share information for these purposes, then none of the information will identify you as an individual and cannot be traced back to you.

How Long do we Keep your Record

The Practice maintains your records in accordance with the **NHS Records Management Code of Practice 2021**.

How we Keep your Personal Information Safe and Secure

To protect personal and special category data, we make sure the information we hold is kept in secure locations and access to information is restricted to authorised personnel only.

Our appropriate technical and security measures include:

- all employees and contractors who are involved in the processing of personal data are suitably trained, on an annual basis, in maintaining the confidentiality and security of the personal data and are under contractual or statutory obligations of confidentiality concerning the personal data.
- robust policies and procedures for example password protection
- technical security measures to prevent unauthorised access
- use of 'user access authentication' mechanisms to make sure all instances of access to any personal data held on clinical systems are auditable against an individual, such as role-based access and Smartcard use to make sure appropriate and authorised access reminding staff of their responsibilities in complying with data protection legislation
- encrypting information transmitted between partners
- implementing and maintaining business continuity, disaster recovery and other relevant policies and procedures
- completion of the Data Security and Protection Toolkit (DSPT) an annual self-assessment requirement that ensure organisation are compliant with the latest data protection and cyber requirements.

- regular audit of policies and procedures to ensure adherence against these criteria

The NHS Digital Code of Practice on Confidential Information applies to all staff who access clinical systems. They are required to protect your information, inform you of how your information will be used, and allow you to decide if and how your information can be shared.

What are your Rights

Under data protection legislation, you have the right:

- **to be informed of the uses of your data:** this enables you to be informed how your data is processed
- **of access:** this enables you to have sight of or receive a copy of the personal information held about you and to check the lawful processing of it
- **to rectification:** this enables you to have any incomplete or inaccurate information held about you corrected
- **to erasure:** this enables you to request we erase personal data about you we hold. This is not an absolute right, and depending on the legal basis that applies, we may have overriding lawful grounds to continue to process your data
- **to restrict processing:** this enables you to ask us to suspend the processing of personal information about you, for example, if you want us to establish its accuracy or the reason for processing it
- **to data portability:** this enables you to transfer your electronic personal information to another party, where appropriate.
- **to object:** this enables you to object to processing of personal data about you on grounds relating to your situation. The right is not absolute, and we may continue to use the data if we can demonstrate compelling legitimate grounds.
- in relation to **automated decision making and profiling:** this enables you to be told if your data is being processed using automated software in relation to automated decision making and profiling note: No automated decision making or profiling is undertaken by the PCN services and its practices.

Please note not all these rights are absolute, please see the practices ROPA for more details

If you wish to exercise your rights in any of the ways described above, you should in the first instance contact the practice manager for your GP practice

Right to Complain

You can get further advice or report a concern directly to the practice manager at your GP practice

You also have the right to contact the UK's data protection supervisory authority (Information Commissioner's Office) by:

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Phone: 0303 123 1113 (local rate) or 01625 545745 (national rate)

Email: [ICO Concerns Handling](#)

Information about the way in which the NHS uses personal information and your rights is published by NHS Digital.

The NHS Constitution

The NHS constitution establishes the principles and values of the NHS in England. It sets out the rights patients, the public and staff are entitled to. These rights cover how patients access health services, the quality of care you will receive, the treatments and programmes available to you, confidentiality, information and your right to complain, if things go wrong.

NHS England

NHS England collects health information from the records health and social care providers keep about the care and treatment they give, to promote health or support improvements in the delivery of care services in England.

Reviews of and changes to this privacy notice

We will review the information contained within this notice regularly and update it as required. We therefore recommend you check this webpage regularly to remain informed about the way in which we use your information.