**Wigton Group Medical Practice**

**Privacy notice**

As data controllers, GPs have fair processing responsibilities under the Data Protection Act and GDPR law 2018. This means ensuring that your personal confidential data (PCD) is handled in ways that are safe, transparent and what you would reasonably expect. Please find documents and links below.

This practice’s primary purpose is to provide the best care possible for you. In order to do this, we need to collect, store and share information about you.

This privacy notice is designed to explain what happens to any personal data that you give us or any information concerning you that is collected by other organisations, for instance, if you attend an Accident and Emergency department. This includes how your data is held and/or processed by us.

This notice includes:

* Who we are and how we use your information
* The kinds of information we hold and how we process them
* The legal grounds for processing your personal data, including when it is shared with others
* What to do if your personal information changes
* The length of time that your information is stored and retained by us
* Information about your rights under the 2018 Data Protection Act incorporating the UK General Data Protection Regulations (GDPR)
* Information about what to do if you have a query or problem

Under the 2018 Data Protection Act incorporating the UK General Data Protection Regulation –(GDPR) the practice is known as the Data Controller. As such we are responsible for keeping your data up to date and accurate, as well as storing it safely and sharing it securely. If you have a problem or a question, you should contact the Deputy Practice Manager, Sharon Nichol, in the first instance. The Act stipulates also that public sector organisations should provide access to an independent Data Protection Officer and their contact details are provided in the summary below.

**The information we hold on you**

Our practice keeps data on you relating to who you are, where you live, your contact details, your family, details of your occupation -if any – and possibly your employers, your habits, your health problems and diagnoses, the reasons you seek help as well at your appointments. Your record also contains details if you have a carer, where you are seen, when you are seen, and who by: as well as all referrals to specialists and other health and social care providers, tests carried out here and in other places, investigations and scans, treatments and outcomes of treatments, your treatment history, the observations and opinions of other health care workers, within and without the NHS as well as comments and aide memoires reasonably made by healthcare professionals in this practice and the Keswick & Solway Primary Care Network who are appropriately involved in your health care. All of this data helps us in providing you with the best possible care and as quickly as possible in an emergency.

All health related data is seen as ‘special category’ or ‘sensitive data’ under the 2018 Data Protection Act which means that it is shared and processed with particular care. This applies to your data whether it is in electronic formats or on paper.

When registering for NHS care, all patients who eligible for NHS care receive a unique NHS Number and are registered on a national database, the database is held by NHS Digital, a national organisation which has legal responsibilities to collect NHS data.

**Why we hold and process your data**

We hold and process your personal data in order to provide you with direct care. Anonymised and pseudonymised patient data, in other words data that cannot be used to identify you is also used to:

* Improve the quality and standard of care that we and other organisations provide
* Researching and developing new treatments
* Developing preventative treatment of illness and disease
* Monitoring standards of patient safety
* Planning future services.

You also have a choice over whether you wish to use your confidential data – i.e. data that CAN be traced back to you for these purposes. If you are content with this then you do not need to do anything. If you are not sure or wish to opt out, please see section on Opting-Out of Research and Planning below.

**Special Provisions during the Covid 19 pandemic**

The NHS faces continued severe pressure during the pandemic. This makes it even more important to share health and care data across relevant organisations.

Using Regulation 3 (4) of the Health Service (Control of Patient Information) Regulations 2002 and related legislation, the Secretary of State for Health has issued a notice (the COPI notice) that requires health organisations including GP surgeries, local authorities and government bodies to share confidential patient information for the duration of the pandemic. There are new services and information flows that have been set up to manage the outbreak. For instance, this practice is part of a Primary Care Network and a GP Federation. As such, it collaborates to deliver COVID vaccinations in this area and is part of a ‘buddy system’ so that if its staff are so affected by the virus, that the practice cannot operate, colleagues from other practices and other organisations can still provide you with care.

All patients registered with a GP have a Summary Care Record (SCR) unless they have chosen not to have one. This record gives professionals in the healthcare system away from your practice access to your information when you need it. If you have previously expressed a preference to only have core information shared in the Summary Care Record or to opt out of the SCR completely. These preferences will be respected. For all other patients the SCR will be used to share additional information as required. New opt-out requests and changes to your opt-out preferences will be suspended and not processed for the duration of the pandemic.

Automated processing of data will be used to identify vulnerable patients and patients needing to be shielded.

NHS England and NHS Improvement and NHSX have developed a single, secure data-store to gather data from across the health and care system to manage and inform the Covid 19 response.

Any data-flows used to share data specifically to manage Covid 19 during the pandemic will cease once the COPI notice is withdrawn.

Because of the importance of sharing data for us all (defined as “public interest” under the 2018 Data Protection Act) any patient opt-out including the National Data Opt-out will not apply during the COPI notice period. It may also take the practice longer to respond to Data Subject Access Requests (DSARs) than the stipulated one calendar month. The Information Commissioner’s Office has recognised the pressure the pandemic has placed upon GP surgeries.

**Who do we share information with**

As GPs, we cannot provide all your treatment ourselves, so we need to delegate this responsibility to others within the practice and with other organisations such as pharmacies or hospitals.

If your care requires treatment outside the practice, we will exchange with those providing such care and treatment whatever information may be necessary to provide you with safe, high quality care. The practice also delivers services and treatment to our patients as part of, and in association with local primary care networks and beyond.

Once you have seen any outside care provider, they will normally send us details of the care they have provided you with, so that we can understand your health and treatment better.

The sharing of personal data, within the practice and with those other organisations involving the practice, such as Primary Care Networks (PCNs) as well as secondary care organisations and social prescribing organisations is assumed and is allowed by law (including the Data Protection Act 2018). However, we will gladly discuss this with you in more detail if you would like to know more. We keep a register of our Information Assets which also sets out a Record of Processing Activity. The majority of patient data processing and storage happens via our EMIS and EMIS Community clinical systems.

We have an overriding responsibility to do what is in your best interests under the 2018 Data Protection Act ‘in performance of a public task’ (see legal bases in the summary below). The Practice team (clinicians, administration and reception staff) only access the information they need to allow them to perform their function and fulfil their roles.  A list of the types of organisation we share with is provided below. This summary also contains details of your rights in relation to your data under the Act and how to exercise them.

We do also share anonymised data across our Primary Care Networks, Cumbria Health on Call, North East and North Cumbria ICB and NHS England. This data is extracted by secure data extraction tools such as EMIS Enterprise and/or Apollo.

This practice does NOT share your data with insurance companies, except by your specific instruction or consent.

However, the practice does outsource the preparation of medical insurance reports and medical reports to a company called iGPR.

Your data is NOT shared or sold for any marketing purpose.

**What patient data is shared about you with NHS England?**

The collection date is still to be confirmed, although when it has been, patient data will be collected from GP medical records about:

* Any living patient registered at a GP practice in England when the collection started – this includes children and adults
* Any patient who died after the data collection started and was previously registered at a GP practice in England when the data collection started



They will not collect your name or where you live. Any other data that could directly identify you, for example NHS number, General Practice Local Patient Number, postcode and date of birth, is replaced with unique codes that are produced by de-identification software before the data is shared with NHS England.

This process is called pseudonymisation and means that no one will be able to directly identify you from the data. The diagram helps to explain what this means. The diagram below helps to explain what this means and using the terms in the diagram, the data we share would be described as de-personalised.

*Image provided by Understanding Patient Data under licence.*

**The data collected by NHS England**

We will share structured and coded data from GP medical records that is needed for specific health and social care purposes as explained above.

Data that directly identifies you as an individual patient, including your NHS number, General Practice Local Patient Number, postcode, date of birth and if relevant date of death, is replaced with unique codes produced by de-identification software before it is sent to NHS England. This means that no one will be able to directly identify you in the data.

NHS England will collect:

* Data on your sex, ethnicity, and sexual orientation
* Clinical codes and data about diagnoses, symptoms, observations, test results, medications, allergies, immunisations, referrals and recalls and appointments including information about your physical, mental, and sexual health
* Data about the staff who have treated you

More detailed information about the patient data collected is contained within the [Data Provision Noticed issued to GP practices](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns/general-practice-data-for-planning-and-research).

NHS England will not collect:

* Your name and address (except for your postcode in unique coded form)
* Written notes (free text) such as the details of conversations with doctors and nurses
* Images, letters and documents
* Coded data that is not needed due to its age – for example medication, referral and appointment data that is over 10 years old
* Coded data that GPs are not permitted to share by law – for example certain codes about IVF treatment and certain information about gender re-assignment

**NHS England legal basis for collecting, analysing and sharing patient data**

When NHSE collects, analyses, publishes and shares patient data, there are strict laws in place that it must follow. Under the UK General Data Protection Regulation (UK GDPR), this includes explaining to patients what legal provisions apply under UK GDPR that allows it to process patient data. The UK GDPR protects everyone's data.

NHSE has been directed by the Secretary of State for Health and Social Care under the [General Practice Data for Planning and Research Directions 2021](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/general-practice-data-for-planning-and-research-directions-2021) to collect and analyse data from GP practices for health and social care purposes including policy, planning, commissioning, public health and research purposes. NHSE is the controller of the patient data collected and analysed under the GDPR jointly with the Secretary of State for Health and Social Care.

All GP practices in England are legally required to share data with NHSE for this purpose under the [Health and Social Care Act 2012](https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted). More information about this requirement is contained in the [Data Provision Notice](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns/general-practice-data-for-planning-and-research) issued by NHSE to GP practices.

NHSE has various powers to publish anonymous statistical data and to share patient data under sections 260 and 261 of the 2012 Act. It also has powers to share data under other Acts, for example the [Statistics and Registration Service Act 2007](https://www.legislation.gov.uk/ukpga/2007/18/contents).

Regulation 3 of the [Health Service (Control of Patient Information) Regulations 2002](https://www.legislation.gov.uk/uksi/2002/1438/contents/made) (COPI) also allows confidential patient information to be used and shared appropriately and lawfully in a public health emergency. The Secretary of State issued legal notices under COPI (COPI Notices) requiring NHSE, arm's-length bodies (such as UK Health Security Agency), local authorities, NHS trusts, ICBs and GP practices to share confidential patient information to respond to the COVID-19 outbreak.

It should be noted that COPI came to an end on 30 June 2022 and was not renewed.

**How NHS England uses patient data**

NHSE will analyse and link the patient data we collect with other patient data we hold to create national data sets and for data quality purposes. NHSE will be able to use the de-identification software to convert the unique codes back to data that could directly identify patients in certain circumstances for these purposes, where this is necessary and where there is a valid legal reason. There are strict internal approvals which need to be in place before NHSE can do this and this will be subject to independent scrutiny and oversight by the [Independent Group Advising on the Release of Data (IGARD](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/independent-group-advising-on-the-release-of-data)).

These national data sets are analysed and used by NHSE to produce national statistics and management information including public dashboards about health and social care which are published. NHSE never publishes any patient data that could identify any individual. All data they publish is anonymous statistical data.

For more information about data NHSE publishes see [Data and Information](https://digital.nhs.uk/data) and [Data Dashboards](https://digital.nhs.uk/dashboards).

**Who does NHS England share patient data with?**

All data that is shared by NHSE is subject to robust rules relating to privacy, security and confidentiality and only the minimum amount of data necessary to achieve the relevant health and social care purpose will be shared.

All requests to access patient data from this collection, other than anonymous aggregate statistical data, will be assessed by NHSE’s [Data Access Request Service](https://digital.nhs.uk/services/data-access-request-service-dars) to make sure that organisations have a legal basis to use the data and that it will be used safely, securely and appropriately.

These requests for access to patient data will also be subject to independent scrutiny and oversight by the [Independent Group Advising on the Release of Data (IGARD)](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/independent-group-advising-on-the-release-of-data). Organisations approved to use this data will be required to enter into a data sharing agreement with NHSE regulating the use of the data.

There are several organisations that are likely to need access to different elements of patient data from the General Practice Data for Planning and Research collection. These include but may not be limited to:

* The Department of Health and Social Care (DHSC) and its executive agencies including UK Health Security Agency (UKHSA) and other government departments
* NHS England
* Primary Care Networks (PCNs) and Integrated Care Boards (ICBs)
* Local Authorities
* Research organisations including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

If the request is approved, the data will either be made available within a secure data access environment within the NHSE infrastructure or, where the needs of the recipient cannot be met this way, as a direct dissemination of data. NHSE plans to reduce the amount of data being processed outside central, secure data environments and increase the data it makes available to be accessed via its secure data access environment.

Data will always be shared in the uniquely coded form (de-personalised data in the diagram above) unless in the circumstances of any specific request it is necessary for it to be provided in an identifiable form (personally identifiable data in the diagram above), for example, when express patient consent has been given to a researcher to link patient data from the General Practice for Planning and Research collection to data the researcher has already obtained from the patient. It is therefore possible for NHSE to convert the unique codes back to data that could directly identify patients in certain circumstances, and where there is a valid legal reason which permits this without breaching the common law duty of confidentiality.

This would include:

* Where the data is needed by a health professional for the patient’s own care and treatment
* Where the patient has expressly consented to this, for example to participate in a clinical trial
* Where there is a legal obligation, for example where there are COPI Notices
* Where approval has been provided by the [Health Research Authority](https://www.hra.nhs.uk/) or the Secretary of State with support from the [Confidentiality Advisory Group (CAG)](https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/) under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) - this is sometimes known as a ‘section 251 approval’

This would mean that the data was personally identifiable in the diagram above. Re-identification of the data would only take place following approval of the specific request through the Data Access Request Service and subject to independent assurance by IGARD and consultation with the Professional Advisory Group which is made up of representatives from the BMA and the RCGP. If patients have registered a national data opt-out this would be applied in accordance with the national data opt-out policy before any identifiable patient data (personally identifiable data in the diagram above) about the patient was shared.

Details of who NHSE has shared data with, in what form and for what purposes are published on its [data release register](https://digital.nhs.uk/services/data-access-request-service-dars/register-of-approved-data-releases).

**Where does NHS England store patient data?**

NHSE only stores and processes patient data for this data collection within the United Kingdom (UK). Fully anonymous data (that does not allow patients to be directly or indirectly identified), for example statistical data that is published, may be stored and processed outside of the UK.

Some of the NHSE processors may process patient data outside of the UK. If they do, they will always ensure that the transfer outside of the UK complies with data protection laws.

**Practice Communication with Patients**

The practice will use your contact details in order to inform you of progress in your treatment or to work with you in managing your health. Because we can communicate and get data to you more quickly and more securely, we prefer to use email and text messaging services. Please ensure that we have your current, up to date, email address and mobile telephone so that we can do this. If you would prefer us NOT to communicate with you in these ways, please let us know.

The practice may use YouTube or similar media in order to communicate with specific groups of patients. Patients will never be asked to pay for such a service, but should be aware that the nature of YouTube or similar is that providers of content may receive remuneration based upon the number of hits that content receives.  If offered such a service, patients can decline or opt-out at any time.

**Safeguarding and the Caldicott Guardian**

The practice is dedicated to safeguarding all its patients, including children and vulnerable adults. This means that information will be shared by the practice in their best interests. Such decisions are the ultimate responsibility of the practice’s Caldicott Guardian. The Caldicott Guardian is the senior person – always a doctor and often a partner within a practice- responsible for protecting the confidentiality of people’s health and care information. The duty to share data for the benefit of individuals is as important as the duty to protect patient confidentiality and actions taken as a result of safeguarding concerns will override data protection. Their decision to share or not to share data is final and there is no appeal process.

**Medical Audits and Medicines Management**

The practice will conduct audits of its services and treatment as well as reviews of medicines prescribed to its patients. Reviews of patient data are necessary to allow us to test and update our services and prescribing to ensure that you receive the most appropriate and cost-effective treatments. These reviews may take the form of internal audits or those conducted by other commissioned healthcare organisations such as North East Commissioning Service (NECs) and Cumbria Health on Call (CHoC).

**Risk Stratification**

Electronic tools of prediction, based upon algorithms and artificial intelligence are used within the NHS to determine a patient’s future risks and treatment needs. Wherever we can, we want to prevent admissions to A&E and secondary care which would be otherwise necessary. Such preventative care may, for instance, use these tools to determine the risk and consequence of a future fall in an elderly patient. Under Covid 19 these tools are being used to identify vulnerable patients and patients who need to be shielded.

However, under the 2018 Data Protection Act, when the COPI notice described above is withdrawn, you do have the right to opt out of having your data processed in such automated ways. If you wish to opt out of this, please contact the practice.

**Research and Planning**

The practice takes part in research that uses anonymised or pseudonymised data. It also takes part in planning at a local, regional and national level. Data which is anonymised or pseudonymised data means that it cannot be traced back to an identifiable individual and is therefore no longer personal data under the 2018 Data Protection Act and thus preserves patient privacy and confidentiality..

[NHS Digital collects pseudonymised patient data on a regular basis and their privacy notice explaining more about how this data is collected and how it is used is available by clicking here](https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research/gp-privacy-notice)

Anonymised or pseudonymised patient data held by the practice may also be used to evaluate present services that provide direct care or to plan future ones within the practice or across the local area.

Identifiable patient data may be used in planning and managing the response of the NHS to the Covid 19 virus due to the overriding priority of serving the national public health interest. This will continue until the COPI notice above is withdrawn.

Sometimes, the practice is contacted to ask whether its patients would consider taking part in research on a particular condition, but where the data used would identify those individuals. In all such cases, identifiable patient data can only be used where patients have given their consent.

**Telephone system**

Our telephone system records all telephone calls. Recordings are retained for 12 months and are used periodically for the purposes of seeking clarification where there is a dispute as to what was said and for staff training. Access to these recordings is restricted to senior staff.

**Organisation website**

Our website does use cookies to optimise your experience. Using this feature means that you have agreed to the use of cookies as required by the EU Data Protection Directive 95/46/EC. You have the option to decline the use of cookies on your first visit to the website. The only website this privacy notice applies to is this organisation’s website.

If you use a link to any other website from the organisation’s website then you will need to read their respective privacy notice. We take no responsibility (legal or otherwise) for the content of other websites.

**Data Opt-Outs and Your Right to Object.**

You cannot opt-out of your data being shared for the purposes of providing you with direct care. You can opt-out of NHS Digital collecting your information, as outlined above, for purposes beyond your direct care; namely, planning and research based on your pseudonymised data.

To do this, you can check your present status and/or change your preferences at [Your NHS Data Matters](https://www.nhs.uk/your-nhs-data-matters) on-line and read the information and follow the instructions if you wish to opt out. This opt-out is recorded against your NHS number on the NHS ‘spine’. The NHS ‘spine’ is administered by NHS Digital.

You can also download a form called a Type 1 opt-out from the NHS Digital website. This form which will be processed at the practice prevents identifiable patient data being shared outside of your practice except where it is being used for purposes of providing you with individual care.

You can also exercise your ‘right to object’ to a specific process involving your data. If you wish to do this for data processed at this practice then you must contact the practice’s Data Protection Officer.

There are some situations where your data will be shared in addition to providing you with direct care. These include:

* Situations where data is needed in the “public interest”, e.g in cases of epidemic where communicable diseases need to be diagnosed and the spread of their infection prevented or controlled;
* To monitor and deliver vaccination programmes;
* Where there is a legal compulsion;
* To manage risks of infection from food or water supplies or the environment.

You can find out more about how your patient information is used at the [Health Research Authority website](https://www.hra.nhs.uk/information-about-patients/) and the [Understanding Patient Data website](https://understandingpatientdata.org.uk/introducing-patient-data)

This practice is compliant with the national data opt-out policy.

**How is your information stored?**

The practice stores the main patient record via a contracted data processor in the cloud. The contracted processor for the practice is Egton Medical Information Systems (EMIS). They can be contacted via EMIS, Rawdon House, Green Lane, Yeadon, Leeds LS19 7BY.

**How long is the information retained?**

The medical record is retained at the patient’s practice for the lifetime of the patient, after which it is sent to Primary Care Services England (PCSE). If you move to another practice your records will be transferred to that practice.

**Summary**

|  |  |
| --- | --- |
| Data Controller | Wigton Group Medical Practice |
| Data Protection Officer | Anna Sives |
| Purpose of Processing your personal information | Direct Care delivered to the individual alone, much of which is provided in the surgery. After a patient agrees to a referral for direct care elsewhere, such as a referral to a specialist in a hospital, necessary and relevant information about the patient, their circumstances and their problem will need to be shared with the other healthcare workers, such as specialist, therapists, technicians etc. The information that is shared is to enable the other healthcare and social care professionals to provide the most appropriate advice, investigations, treatments, therapies and or care. |
| Lawful Basis for Processing your personal information | The processing of personal data in the delivery of direct care and for providers’ administrative purposes in this surgery and in support of direct care elsewhere is supported under the following Article 6 and 9 conditions of the GDPR:Article 6 (1) (c) – the processing is necessary for compliance with a legal obligation to which the controller (the practice is subject) and/orArticle 6(1)(e) ‘…the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority…’.Health data is defined as a special kind of personal data and is also processed by the practice underArticle 9(2)(h) ‘necessary for the purposes of preventative 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..’The sharing of your personal data also takes place in accordance with the common law duty of confidentiality. Performance of this duty does not require consent from the patient where the proposed use of their data is either for individual care or in the public interest. |
| Recipient or categories of recipients of your personal data | The data will be shared with health and care professionals and support staff in this surgery and at hospitals, diagnostic and treatment centres who contribute to your personal care. GPs, Hospitals, Primary Care Network, Local GP provider organisation, NHS Commissioning Support Units, Social Care Services, Health and Social Care Information Centre (HSCIC), Clinical Excellence Group, Community Pharmacists, District Nurses, Independent Contractors such as dentists, opticians, pharmacists, Private Sector Providers, Voluntary Sector Providers, Ambulance Trusts, Mental Health Trusts, Out of hours organisation, Integrated commissioning boards, Local Authorities, Education Services, Fire and Rescue Services, Police & Judicial Services, The Child Health Information Service, Substance Misuse Remote Workers, Coroner’s office, Providers Voluntary Sector, Private Sector Providers, Social Prescribers. Many organisations across North East and North Cumbria share an aggregated summary view of your data, held in a secure Health Information Exchange and using a Local Health Care Exemplar format known as the Great North patient record, in order to make quicker and better informed decisions in providing you with care. This practice is also part of Keswick & Solway Primary Care Network designed to bring together a number of service providers to help patients with more than one need. |
| Your right to object | You have the right to object to some or all of the information being processed, which is detailed under Article 21. Exercising your right to object may well prevent the referral or course of treatment from going ahead. Please contact the Data Protection Officer.You should be aware that this is a right to raise an objection that is not the same as having an absolute right to have your wishes granted in every circumstance. |
| Your right to access and correction | You have the right to access your data and to have any inaccuracies corrected. There is no right to have medical records deleted except when ordered by a court of Law. |
| How long do we hold your personal data for? | We retain your personal data in line with both national guidance and law, which can be found at [Records Management Code of Practice](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/records-management-code-of-practice-for-health-and-social-care-2016) |
| Your right to complain | If you have a question or wish to complain about the use of your data, you should approach the Practice Manager or contact the Data Protection Officer.The use of personal data is overseen by the Information Commissioners Office, often known as the ICO. If you wish to complain or raise a concern with the ICO, [they can be contacted via their website](https://ico.org.uk/). Or you can also call their helpline Tel: 0303 123 1113 (local rate)01625 545 745 (national rate)Or you can write to them at;The ICO, Wycliffe House, Water Ln, Wilmslow SK9 5AF |

**Data Processor Update**

This practice acts as Data Controller for your data. It uses a number of suppliers as Data Processors. These suppliers may be procured, national regionally or locally and support the practice by providing various clinical services under instruction.

Patients receiving warfarin treatment are monitored by a system called INR Star. This system is owned by LumiraDX Care Solutions.

LumiraDx Care Solutions are planning to migrate INRstar from its current location to a new Cloud-First technology. During this move, the data residency will remain in England in a UK Government approved data centre. There is no threat to patient confidentiality and data will not be modified in any way, and the way it is processed will remain the same following the migration. [Lumira DX Care Solutions privacy policy and data protection impact assessment can be found by clicking here](https://lumiradxcaresolutions.com/legal/%22%20%5Ct%20%22_blank)

The practice outsources preparation of medical reports for personal and insurance purposes and subject access reports. We use a processor, iGPR Technologies Limited (“iGPR”), to assist us with responding to report requests relating to your patient data, such as subject access requests that you submit to us (or that someone acting on your behalf submits to us) and report requests that insurers submit to us under the Access to Medical Records Act 1988 in relation to a life insurance policy that you hold or that you are applying for. iGPR manages the reporting process for us by reviewing and responding to requests in accordance with our instructions and all applicable laws, including UK data protection laws. The instructions we issue to iGPR include general instructions on responding to requests and specific instructions on issues that will require further consultation with the GP responsible for your care.

National Registries

National Registries such as the Learning Disabilities Register and cervical screening have statutory permission under Section 251 of the NHS Act 2006, to collect and hold service user identifiable information without the need to seek informed consent from each individual service user.

**What to do if you have any questions**

Should you have any questions about our privacy policy or the information we hold about you, you can:

1. Contact the organisation via the contact form on our practice website, GP practices are data controllers for the data they hold about their patients (for more information, refer to the [BMA guidance](https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers) on this subject)

1. Write to the Data Protection Officer (DPO) Ms Anna Sives
2. Ask to speak to the Practice Manager, Anna Sives or their deputy, Kerry Lawrence.

**Wigton Group Medical Practice Employee Privacy Notice**

Wigton Group Medical Practice gathers and processes personal data relating to its employees to enable us to run the business and manage our relationship with you.  We are committed to being open and transparent about how we gather and use that data and to meeting our data protection obligations.

This privacy notice applies to personal information processed by or on behalf of Wigton Group Medical Practice.

This notice explains:

* Who we are, how we use your information and our data protection officer (DPO)
* What kind of personal information about you we process?
* What the legal grounds are for our processing of your personal information (including when we share it with others)
* What you should do if your personal information changes
* For how long your personal information is retained by us
* What your rights are under data protection laws

The UK 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 entered 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 (DPA2018), the organisation responsible for your personal data is Wigton Group Medical Practice.

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**

Wigton Group Medical Practice will be what is known as the ‘controller’ of the personal data you provide to us. Upon commencement of employment with the organisation you will be asked to supply the following personal information:

* Name
* Address
* Telephone numbers
* Email address
* Date of birth
* Gender
* Marital status and family details
* National insurance number
* Bank details
* Emergency contact information
* Health information
* Vaccination and immunisation status/information
* Recruitment information such as your application form and CV, references, qualifications and membership of any professional bodies and details of any pre-employment assessments
* Information about your contract of employment (or services) including start and end dates of employment, role and location, working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
* Your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
* Information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
* Information relating to your performance and behaviour at work
* Training records
* Electronic information in relation to your use of IT systems/swipe cards/telephone systems
* Your images (whether captured on CCTV, by photograph or video)

The information that we ask you to provide to the organisation is required by the business for the following reasons:

* In order for us to pay your salary
* In order for us to contact you out of hours if required
* To provide you with organisation information via email and post if required
* To have the ability to contact your emergency contacts if necessary
* To ensure we are able to inform the emergency services if your health is compromised
* To ensure that we can provide any reasonable adjustments as necessary
* To comply with payroll, auto-enrolment and RTI responsibilities

The organisation may collect this information in a variety of ways, for example from application forms, CVs or resumes, obtained from your passport or other identity documents such as your driving licence, from forms completed by you at the start of or during employment (such as pensions benefit nomination forms), from correspondence with you or through interviews, meetings or other assessments.

This personal data might be provided to us by you or someone else (such as a former employer, your doctor or a credit reference agency and information from criminal records checks permitted by law) or it could be created by us.

Your personal data will be stored in a range of different places including in your personnel file, in the organisation’s HR management systems and in other IT systems (including the organisation’s email system).

Throughout your employment we will collect data and add to your electronic personnel file i.e., appraisal paperwork, communications, absence information and changes to personnel data.

**Special categories of personal data**

Some special categories of personal data, such as information about health or medical conditions, are processed to carry out employment law obligations (such as those in relation to employees with disabilities).

Where the organisation processes other special categories of personal data, such as information about ethnic origin, sexual orientation or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees which can be withdrawn at any time. Employees are entirely free to decide whether to provide such data and there are no consequences of failing to do so.

**How do we lawfully use your data?**

We need to know your personal, sensitive and confidential data in order to employ you, under the General Data Protection Regulation we will be lawfully using your information in accordance with:

* Article 6, (b) Necessary for performance of/entering into contract with you
* Article 9(2) (b) Necessary for controller to fulfil employment rights or obligations in employment

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

**How do we maintain the confidentiality of your record?**

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

* Data Protection Act 2018
* The UK General Data Protection Regulations
* Human Rights Act 1998
* Common Law Duty of Confidentiality

**NHS Codes of Confidentiality, Information Security and Records Management**

We will only ever use or pass on information about you to others who 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) or where the law requires information to be passed on.

Our policy is to respect the privacy of our staff and to maintain compliance with the UK General Data Protection Regulation (UK GDPR) and all UK specific data protection requirements. Our policy is to ensure all personal data related to our staff will be protected.

All employees and sub-contractors engaged by Wigton Group Medical Practice are asked to sign a confidentiality agreement. The organisation will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Wigton Group Medical Practice an appropriate contract (art. 24-28) will be established for the processing of your information.

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

**Where do we store your information electronically?**

All the personal data we process is processed by our organisation in the UK.

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.  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:

* Primary Care Networks
* Integrated Care Systems
* NHS England (NHSE) and NHS Digital (NHSD)
* Local authorities
* CQC
* Private sector providers providing employment services
* Other ‘data processors’ which you will be informed of

**Sharing your personal data**

Your information may be shared internally including with members of the Wigton Group Medical Practice management team (including payroll), your line manager, GP Partners and IT staff if access to the data is necessary for performance of their roles.

Sometimes we might share your personal data with other organisations within our group or our contractors to carry out our obligations under our contract with you or for our legitimate interests, for example to obtain employment background checks from third-party providers and obtain necessary criminal records checks from the Disclosure and Barring Service, payroll, the provision of benefits and the provision of occupational health services.

The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The organisation will not transfer your data to countries outside the European Economic Area.

You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

We may also use external companies to process personal information such as for payroll purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure.  All employees and sub-contractors engaged by Wigton Group Medical Practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for the organisation, an appropriate contract (art. 24-28) will be established for the processing of your information.

**Who is the data controller?**

Wigton Group Medical Practice is registered as a data controller under the Data Protection Act 2018. Our registration number is Z5521099 and our registration can be viewed online in the public register at [www.ico.gov.uk](https://ico.org.uk/ESDWebPages/Search). This means we are responsible for handling your personal information and collecting and storing it appropriately.

We may also process your information for a particular purpose and therefore we may also be data processors. The purposes for which we use your information are set out in this privacy notice.

**How long do we keep your personal 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: [NHSX – Records Management Code of Practice 2020](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/)

**How can you access, amend or 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. For further information about this, please contact the Practice manager.  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 to resolve any issues that 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 is 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.

**Your rights as an employee**

Data Subject Access Requests (DSAR): You have a right under the data protection legislation to request access to view or to obtain copies of what information this organisation holds about you and to have it amended should it be inaccurate. To request this, you need to do the following:

Your request should be made to Anna Sives, Data protection Officer, Wigton Group Medical Practice.

There is no charge to have a copy of the information held about you. However, we may, in some limited and exceptional circumstances, have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive

We are required to provide you with information within one month. We would ask therefore that any requests you make are in writing and it is made clear to us what and how much information you require

You will need to give adequate information (for example full name, address, date of birth and details of your request) so that your identity can be verified, and your records located

**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). Wigton Group Medical Practice will from time to time ask you to confirm that the information we currently hold is accurate and up to date.

**What to do if you have any questions**

Should you have any questions about this privacy policy or the information we hold about you, you can:

Contact the organisation via email at nencicb-cu.wigton@nhs.net. For the attention of data protection officer.

Write to the data protection officer at Wigton Group Medical Practice, Southend, Wigton, CA7 9QD.

**Objections or complaints**

In the unlikely event that you are unhappy with any element of our data processing methods, do please contact the Practice manager at Wigton Group Medical Practice in the first instance. If you feel that we have not addressed your concern appropriately, you have the right to lodge a complaint with the ICO. For further details, visit [ico.gov.uk](https://www.ico.gov.uk/) and select “Raising a concern” or telephone: 0303 123 1113

The Information Commissioner’s Office is the regulator for the General Data Processing Regulations and offers independent advice and guidance on the law and personal data including your rights and how to access your personal information.

**Changes to our privacy policy**

We regularly review our employee privacy policy, and any updates will be published to reflect the changes. This policy is to be reviewed annually. (Reviewed Feb 2024)

In the UK, your rights arise from the General Data Protection Regulation as retained, amended EU law, and the supervisory authority is the UK Information Commissioner (<https://ico.org.uk/>).