**NHS Digital Data Collection from the Practice**

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

GP practices already share patient data for these purposes, but this new data collection will be more efficient and effective.

This means that GPs can get on with looking after their patients, and NHS Digital can provide controlled access to patient data to the NHS and other organisations who need to use it, to improve health and care for everyone.

Contributing to research projects will benefit us all as better and safer treatments are introduced more quickly and effectively without compromising your privacy and confidentiality.

NHS Digital has engaged with the British Medical Association (BMA), Royal College of GPs (RCGP) and the National Data Guardian (NDG) to ensure relevant safeguards are in place for patients and GP practices.

**NHS Digital purposes for processing patient data**

Patient data from GP medical records kept by GP practices in England is used every day to improve health, care and services through planning and research, helping to find better treatments and improve patient care. The NHS is introducing an improved way to share this information - called the General Practice Data for Planning and Research data collection.

NHS Digital will collect, analyse, publish and share this patient data to improve health and care services for everyone. This includes:

• informing and developing health and social care policy

• planning and commissioning health and care services

• taking steps to protect public health (including managing and monitoring the coronavirus pandemic)

• in exceptional circumstances, providing you with individual care

• enabling healthcare and scientific research

Any data that NHS Digital collects will only be used for health and care purposes. It is never shared with marketing or insurance companies.

**What patient data NHS Digital collect**

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

While 1 September has been seen by some as a cut-off date for opt-out, after which data extraction would begin, Government has stated this will not be the case and data extraction will not commence until NHS Digital have met the tests.

The NHS is introducing three changes to the opt-out system which mean that patients will be able to change their opt-out status at any time:

• Patients do not need to register a Type 1 opt-out by 1 September to ensure their GP data will not be uploaded

• NHS Digital will create the technical means to allow GP data that has previously been uploaded to the system via the GPDPR collection to be deleted when someone registers a Type 1 opt-out

• The plan to retire Type 1 opt-outs will be deferred for at least 12 months while we get the new arrangements up and running, and will not be implemented without consultation with the RCGP, the BMA and the National Data Guardian

We 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, full postcode and date of birth, is replaced with unique codes which are produced by de-identification software before the data is shared with NHS Digital.

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



Image provided by Understanding Patient Data under licence.

NHS Digital will be able to use the same software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. Only NHS Digital has the ability to do this. This would mean that the data became personally identifiable data in the diagram above. An example would be where you consent to your identifiable data being shared with a research project or clinical trial in which you are participating, as they need to know the data is about you.

More information about when we may be able to re-identify the data is in the who we share your patient data with section below.

The NHS Digital programme will be providing further information as the programme progresses. In the meantime, if you have any questions, you can contact the programme at enquiries@nhsdigital.nhs.uk

The NHS Digital web pages also provide further information at <https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research#additional-information-for-gp-practices>

**The Data NHD Digital collect**

We will only collect structured and coded data from patient medical records that is needed for specific health and social care purposes explained above.

Data that directly identifies you as an individual patient, including your NHS number, General Practice Local Patient Number, full 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 Digital. This means that no one will be able to directly identify you in the data.

NHS Digital will be able to use the software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. This would mean that the data became personally identifiable in the diagram above. It will still be held securely and protected, including when it is shared by NHS Digital.

**NHS Digital 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 staff who have treated you

More detailed information about the patient data we collect is contained in the Data Provision Notice issued to GP practices.

**NHS Digital Does 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

**Opting out of NHS Digital collecting your data (Type 1 Opt-out)**

If you do not want your identifiable patient data (personally identifiable data in the diagram above) to be shared outside of your GP practice for purposes except for your own care, you can register an opt-out with your GP practice. This is known as a Type 1 Opt-out.

Type 1 Opt-outs were introduced in 2013 for data sharing from GP practices, but may be discontinued in the future as a new opt-out has since been introduced to cover the broader health and care system, called the National Data Opt-out. If this happens people who have registered a Type 1 Opt-out will be informed. More about National Data Opt-outs is in the section Who we share patient data with.

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-out in line with current policy. If this changes patients who have registered a Type 1 Opt-out will be informed.

If you do not want your patient data shared with NHS Digital, you can register a Type 1 Opt-out with your GP practice. You can register a Type 1 Opt-out at any time. You can also change your mind at any time and withdraw a Type 1 Opt-out.

Data sharing with NHS Digital will start on 1 September 2021.

If you have already registered a Type 1 Opt-out with your GP practice your data will not be shared with NHS Digital.

If you wish to register a Type 1 Opt-out with your GP practice before data sharing starts with NHS Digital, this should be done by returning this form to your GP practice. If you have previously registered a Type 1 Opt-out and you would like to withdraw this, you can also use the form to do this. You can send the form by post or email to your GP practice or call 0300 3035678 for a form to be sent out to you.

If you register a Type 1 Opt-out after your patient data has already been shared with NHS Digital, no more of your data will be shared with NHS Digital. NHS Digital will however still hold the patient data which was shared with us before you registered the Type 1 Opt-out.

If you do not want NHS Digital to share your identifiable patient data (personally identifiable data in the diagram above) with anyone else for purposes beyond your own care, then you can also register a National Data Opt-out. There is more about National Data Opt-outs and when they apply in the National Data Opt-out section below.

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

When we collect, analyse, publish and share patient data, there are strict laws in place that we must follow. Under the UK General Data Protection Regulation (GDPR), this includes explaining to you what legal provisions apply under GDPR that allows us to process patient data. The GDPR protects everyone's data.

NHS Digital has been directed by the Secretary of State for Health and Social Care under the 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.

NHS Digital 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 NHS Digital for this purpose under the Health and Social Care Act 2012 (2012 Act). More information about this requirement is contained in the Data Provision Notice issued by NHS Digital to GP practices.

NHS Digital 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.

Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) also allow confidential patient information to be used and shared appropriately and lawfully in a public health emergency. The Secretary of State has issued legal notices under COPI (COPI Notices) requiring NHS Digital, NHS England and Improvement, arm's-length bodies (such as Public Health England), local authorities, NHS trusts, clinical commissioning groups and GP practices to share confidential patient information to respond to the COVID-19 outbreak. Any information used or shared during the COVID-19 outbreak will be limited to the period of the outbreak unless there is another legal basis to use confidential patient information.

 The legal basis under UKGDPR for General Practice Data for Planning and Research

**How NHS Digital use patient data**

NHS Digital 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.

NHS Digital will be able to use the de-identification software to convert the unique codes back to data that could directly identify you 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 we 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 NHS Digital to produce national statistics and management information, including public dashboards about health and social care which are published. We never publish any patient data that could identify you. All data we publish is anonymous statistical data.

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

We may also carry out analysis on national data sets for data quality purposes and to support the work of others for the purposes set out in Our purposes for processing patient data section above.

**Who NHS Digital share patient data with**

All data which is shared by NHS Digital 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 NHS Digital’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 NHS Digital regulating the use of the data.

There are a number of organisations who 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 and its executive agencies, including Public Health England and other government departments

• NHS England and NHS Improvement

• primary care networks (PCNs), clinical commissioning groups (CCGs) and integrated care organisations (ICOs)

• 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 NHS Digital infrastructure, or where the needs of the recipient cannot be met this way, as a direct dissemination of data. We plan to reduce the amount of data being processed outside central, secure data environments and increase the data we make available to be accessed via our secure data access environment. For more information read about improved data access in [improving our data processing services.](https://digital.nhs.uk/data-and-information/data-insights-and-statistics/improving-our-data-processing-services)

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 NHS Digital to convert the unique codes back to data that could directly identify you 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 was needed by a health professional for your own care and treatment

• where you have expressly consented to this, for example to participate in a clinical trial

• where there is a legal obligation, for example where the COPI Notices apply - see Our legal basis for collecting, analysing and sharing patient data above for more information on this

• 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 you 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 you was shared. More about the National Data Opt-out is in the section below.

Details of who we have shared data with, in what form and for what purposes are published on our [data release register.](https://digital.nhs.uk/services/data-access-request-service-dars/data-uses-register)

**Where NHS digital stores patient data**

NHS Digital only stores and processes patient data for this data collection within the United Kingdom (UK).

Fully anonymous data (that does not allow you to be directly or indirectly identified), for example statistical data that is published, may be stored and processed outside of the UK. Some of our processors may process patient data outside of the UK. If they do, we will always ensure that the transfer outside of the UK complies with data protection laws.

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

All the personal data we process is processed by our staff in the UK however for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

No 3rd parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place 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.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations;

• NHS Trusts / Foundation Trusts

• GP’s

• Primary Care Network

• NHS Commissioning Support Units

• Independent Contractors such as dentists, opticians, pharmacists

• Private Sector Providers

• Voluntary Sector Providers

• Ambulance Trusts

• Clinical Commissioning Groups

• Social Care Services

• NHS England (NHSE) and NHS Digital (NHSD)

• Multi Agency Safeguarding Hub (MASH)

• Local Authorities

• Education Services

• Fire and Rescue Services

• Police & Judicial Services

• Voluntary Sector Providers

• Private Sector Providers

• Other ‘data processors’ which you will be informed of

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

**Computer System**

This practice operates a Clinical Computer System 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.

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisation (above). Wherever possible, their staff will ask your consent before your information is viewed.

**Shared Care Records**

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems. You can opt out of this sharing of your records with our partners at anytime if this sharing is based on your consent.

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

**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.

**How long will we store your information?**

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records management code of practice for health and social care and national archives requirements.

More information on records retention can be found online at (<https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016>)

**How can you access, amend move the personal data that you have given to us?**

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

Right to object: If we are using your data and you do not agree, you have the right to object. We will respond to your request within one month (although we may be allowed to extend this period in certain cases). This is NOT an absolute right sometimes we will need to process your data even if you object.

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 send you information about us or matters you may be interested in), 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 one month (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 need to keep a note of your name/ other basic details on our register of individuals who would prefer not to be contacted. This enables us to avoid contacting you in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP to GP data transfer and transfer of your hard copy notes.

**Primary Care Network**

The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces which ease the pressure of GP’s, leaving them better able to focus on patient care.

This practice is a member of Rushcliffe PCN. Other members of the network are:

Belvoir Health Group (Bingham, Cotgrave & surrounding villages), East Bridgford Medical Practice, Radcliffe-on-Trent Health Centre, St Georges (West Bridgford) , Orchard Surgery (Kegworth), Castle Health Care (West Bridgford), Musters Medical Practice (West Bridgford), West Bridgford Medical Practice, Ruddington Medical Practice.

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

**Service Evaluation**

The PCN carries out service evaluations in order to improve the quality and accessibility of primary care services. This may be carried out in a number of 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. 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.

As part of this programme, personal data about your health care will have all identifiers removed (like your name or NHS Number) and replaced with a code which will be linked to information about care received in different health care settings. 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.

As part of this programme your GP and other care providers will send the information they hold on their systems to the North Of England Commissioning Support Unit (NECS). NECS are part of NHS England. More information can be found here https://www.necsu.nhs.uk

NECS will link all the information together. Your GP and other care providers will then review this information and make decisions about the whole population or particular patients that might need additional support. NECS work in partnership with a company called Optum to help them with this work. Both NECS and Optum are legally obliged to protect your information and maintain confidentiality in the same way that your GP or hospital provider is. More information about Optum can be found here www.optum.co.uk.

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.

The PHM project is time-limited to 22 weeks. Once the project has completed all de-identified , information processed by NECS / Optum will be securely destroyed. This will not affect any personal information held by your GP or other health or social care providers.

**Access to your personal information**

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 the surgery 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 the Practice. (For information from a hospital or other Trust/ NHS organisation you should write direct to them.

• There is no charge to have a copy of the information held about you

• We are required to provide you with information within one month

• You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located information we hold about you at any time.

**What should you do if your personal information changes?**

You should tell us so that we can update our records please contact the Practice Manager as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

**Online Access**

You may ask us if you wish to have online access to your medical record. However, there will be certain protocols that we have to follow to give you online access, including written consent and the production of documents that prove your identity.

Please note that when we give you online access, the responsibility is yours to make sure that you keep your information safe and secure if you do not wish any third party to gain access.

Third parties mentioned on your medical record

Sometimes we record information about third parties mentioned by you to us during any consultation, or contained in letters we receive from other organisations. We are under an obligation to make sure we also protect that third party’s rights as an individual and to ensure that references to them which may breach their rights to confidentiality, are removed before we send any information to any other party including yourself.

The NHS wants to give people better ways to see their personal health information online. We know that people want to be able to access their health records. It can help you see test results faster. It also lets you read and review notes from your appointments in your own time.

From 01/112022 we’re now letting you see all the information within your health record automatically. If you are over 16 and have an online account, such as through the [NHS App](https://digital.nhs.uk/services/data-access-request-service-dars/data-uses-register), NHS website, or another online primary care service, you will now be able to see all future notes and health records from your doctor (GP). Some people can already access this feature, this won’t change for you.

This means that you will be able to see notes from your appointments, as well as test results and any letters that are saved on your records. This only applies to records from your doctor (GP), not from hospitals or other specialists. You will only be able to see information from [insert date that your practice will make the change]. For most people, access will be automatic, and you won’t need to do anything.

Your doctor (GP) may talk to you to discuss test results before you are able to see some of your information on the app. Your doctor (GP) may also talk to you before your full records access is given to make sure that having access is of benefit to you. There might be some sensitive information on your record, so you should talk to your doctor if you have any concerns.

These changes only apply to people with online accounts. If you do not want an online account, you can still access your health records by requesting this information through reception. The changes also only apply to personal information about you. If you are a carer and would like to see information about someone you care for, speak to reception staff.

The NHS App, website and other online services are all very secure, so no one is able to access your information except you. You’ll need to make sure you protect your login details. Don’t share your password with anyone as they will then have access to your personal information.

If you do not want to see your health record, or if you would like more information about these changes, please speak to your GP or reception staff.

**Our website**

The only website this Privacy Notice applies to is the Surgery’s website. If you use a link to any other website from the Surgery’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.

The Surgery’s website uses cookies. For more information on which cookies we use and how we use them, please see our Cookies Policy.

**CCTV recording**

CCTV is installed on our practice premises covering both the external area of the building and the internal area excluding consulting rooms. Images are held to improve the personal security of patients and staff whilst on the premises, and for the prevention and detection of crime. The images are recorded onto an integral hard drive of the equipment and are overwritten on a rolling basis. Viewing of these digital images is password protected and controlled by the Practice Manager.

**Telephone system**

Our telephone system may record some telephone calls. Recordings are retained for up to three years, 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 named senior staff.

**Medical Examiner Service**

Following the death of any patients of Village Health Group we are now obliged to inform Nottinghamshire NHS Trust, Medical Examiner Service.

Medical examiner offices at acute trusts now provide independent scrutiny of non-coronial deaths occurring in acute hospitals. The role of these offices is now being extended to also cover deaths occurring in the community.

Medical examiner offices are led by medical examiners, senior doctors from a range of specialties including general practice, who provide independent scrutiny of deaths not taken at the outset for coroner investigation. They put the bereaved at the centre of processes after the death of a patient, by giving families and next of kin an opportunity to ask questions and raise concerns. Medical examiners carry out a proportionate review of medical records, and liaise with doctors completing the Medical Certificate of Cause of Death (MCCD).

The Practice will share any patient with the service upon request.

**Objections / Complaints**

Should you have any concerns about how your information is managed at the GP, please contact the GP Practice Manager or the Data Protection Officer as above. If you are still unhappy following a review by the GP practice, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

Information Commissioner:

Wycliffe house

Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 01625 545745

<https://ico.org.uk/>

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared, then please contact the Practice Data Protection Officer.

If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as below.

**Data Protection Officer:**

The Practice Data Protection Officer is Paul Couldrey of PCIG Consulting Limited. Any queries regarding Data Protection issues should be addressed to him at: -

Email: Couldrey@me.com

Postal: PCIG Consulting Limited

 7 Westacre Drive

 Quarry Bank

 Dudley

 West Midlands

 DY5 2EE

**Changes:**

It is important to point out that we may amend this Privacy Notice from time to time. If you are dissatisfied with any aspect of our Privacy Notice, please contact the Practice Data Protection Officer.