

KINGSBRIDGE MEDICAL PRACTICE

Data Protection Privacy Notice for Patients

Introduction:

This privacy notice lets you know what happens to any personal data that you give to us, or any that we may collect from or about you.

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

This Notice explains

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

The General Data Protection Regulation (GDPR) became law on 25th May 2018. This is a single EU-wide regulation on the protection of confidential and sensitive information, the DPA 2018 deals with elements of UK law that differ from the European Regulation. These came into force in the UK on the 25th May 2018, repealing the Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"), and the Data Protection Act 2018 (currently in Bill format before Parliament) the practice responsible for your personal data is Kingsbridge 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.

Kingsbridge Medical Practice will be what's known as the 'Controller' of the personal data you provide to us.

We collect basic personal data about you which does not include any special types of information or location-based information. This does however include name, address, contact details such as email and mobile number etc. For the purposes of providing healthcare services we may contact you via a variety of communication routes e.g. face to face, letters, via telephone, text or SMS messaging and email.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious belief (if required in a healthcare setting) ethnicity, and sex during the services we provide to you and or linked to your healthcare through other health providers or third parties.

Why do we need your information?

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (e.g. NHS Trust, GP Surgery, Walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

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

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

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

How do we lawfully use your data?

We need to know your personal, sensitive and confidential data in order to provide you with Healthcare services as a General Practice, under the General Data Protection Regulation we will be lawfully using your information in accordance with: -

Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;"

Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

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

NHS Digital

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

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

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 a number of sources including NHS Trusts and from this GP Practice. A risk score is then arrived at through an analysis of your de-identified information is only provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness. If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way.

Medicines Management

The Practice may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments.

Patient Communication

The Practice will use your name, contact details and email address to inform you of NHS services, or to provide you with health/information to manage your healthcare or information about the management of the NHS. There may be occasions where authorised research facilities would like you to take part in research with regard to your particular health issues and to try to improve your health. Your contact details may be used to invite you to receive further information about such research opportunities.

Safeguarding

The Practice is dedicated to ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied. Our legal basis for processing for the General Data Protection Regulation (GDPR) purpose is:

Article 6(1)(e) '...exercise of official authority...'

For the processing of special categories data, the basis is:

Article 9(2)(b) ...'processing is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment and social security and social protection law ...'

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is necessary or possible to obtain to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

The Practice will either receive or collect information when someone contacts us with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

The information is used by the Practice when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals.

Research

Clinical Practice Research Datalink (CRPD) collects pre-identified patient data from a network of GP

practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research at any time, full details can be found here:

<https://cprd.com/transparency-information>

CPRD do not hold or process personal data on patients. However, NHS Digital may process 'personal data' for them as an accredited 'safe haven' or 'trusted third-party' within the NHS when linking GP data with data from other sources. The legal basis for processing this data is:

Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) ...'public interest in the area of public health ...'

Medical research and statistics: Article 6(e) and Article 9(2)(j) ...'public interest and scientific research purposes ...'

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

National Diabetes Prevention Programme

The practice shares data on eligible patients with the NHS Diabetes Prevention Programme, a joint initiative between NHS England, Public Health England and Diabetes UK. This service is provided by Ingeus, who ensure they adopt enhanced security requirements in line with national standards. The purpose of the programme is to deliver behavioural and lifestyle intervention services for people who have already been identified with non-diabetic hyperglycaemia, and who are therefore at high risk of developing Type 2 Diabetes. The legal basis that allows the practice to do this is direct care as detailed under articles 6 and 9 of the DPA18/GDPR as detailed earlier.

Third Party Processors

In order to deliver the best possible service, the Practice will share data (where required) with other NHS bodies such as other GP Practices and hospitals. In addition the Practice will use carefully selected third party 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 and support, including our core clinical systems; systems which manage patient facing services (such as our website and services accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.
- Deliver services e.g. if we were to arrange delivery of medicines to you
- Payment providers e.g. if you were paying for a prescription or services such as travel vaccinations

How do we maintain the confidentiality of your records?

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

- Data Protection Act 2018
- The General Data Protection Regulations 2016
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality, Information Security and Records Management
- Information: To Share or Not to Share Review

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), where the law requires information to be passed on and / or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

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

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Kingsbridge 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.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always contact you to gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information to

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

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.

This information is not shared with third parties or used for any marketing and you can unsubscribe at

any time via phone, email or by informing the practice Data Protection Officer as below.

National Data Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning. You can opt-out of sharing our confidential patient information for this purpose at any time. There may still be times when your information is used however, e.g. during an epidemic where there might be a risk to you or other people's health. You can also still consent to take part in a specific research project.

Choosing to opt out will not affect your care and treatment. Your confidential patient information will still be used for your individual care and you will still be invited for screening services.

You do not need to do anything if you are happy about using your patient information in this way. If you do wish to opt out this can be done securely online or through a telephone service as detailed below:

www.nhs.uk/your-nhs-data-matters

Telephone: 0300 303 5678

Where do we store your information electronically?

All the personal data we hold 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 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.

EMIS Web

The Practice uses a clinical system provided by a data processor called EMIS. With effect from 10th June 2019, EMIS will start storing EMIS web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services (AWS).

The data will remain in the UK at all times 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 clients (including the NHS), and it offers the very highest levels of security and support.

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
- GPs
- 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)
- 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.

The Practice operates a clinical computer system (EMIS WEB) 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 trusted organisations. Where 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 when they are involved with looking after you, we will share information to other systems. The general principle is that information is passed to these systems unless you request this does not happen, but that system users should ask for your consent before viewing your record.

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 Kingsbridge Medical Practice an appropriate contract (art 24-28) will be established for the processing of your information.

Sharing your information without consent

We will normally ask for your consent, but there are times when we may be required by law to share your information without consent, for example:

- Where there is a risk of serious harm or abuse to you or other people
- 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 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. To get in touch about these, please contact us. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

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

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project), or consent to market to you, you may withdraw your consent at any time.

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

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

Access to 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 the hospital you should write direct to them
- There is no charge to have a copy of the information held about you
- We are required to respond to you 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.

What should you do if your personal information changes?

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

Objections / Complaints

Should you have any concerns about how your information is managed at the Practice, please contact the Practice Manager or the Data Protection Officer as below. If you are still unhappy following a review by the Practice, you have a right to complain to a UK Supervisory Authority as below:

Information Commissioner:
Wycliffe house
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545745
www.informationcommissioner.gov.uk

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

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

Data Protection Officer:

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

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

Changes:

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