Version 1 – April 2018

GP Practice Privacy Notice

Protecting Your Privacy

Introduction

This privacy notice explains in detail why we use your personal data which we, the GP practice, (Data Controller), collects and processes about you. A Data Controller determines how the data will be processed and used with the GP practice and with others who we share this data with. We are legally responsible for ensuring that all personal data that we hold and use is done so in a way that meets the data protection principles under the General Data Protection Regulation (GDPR) and Data Protection Act 2018. This notice also explains how we handle that data and keep it safe.

We will continually review and update this privacy notice to reflect changes in our services and to comply with changes in the Law. When such changes occur, we will revise the last updated date as documented in the Version Control Section of this document.

What we do and how we use your personal data?

We are here to provide care and treatment to you as our patients. In order to do this, the GP practice keeps personal data about you such as your name, address, date of birth, telephone numbers, email address, NHS Number etc and your health and care information (which is known as a special category of information under the General Data Protection Regulation (GDPR). Information is needed so we can provide you with the best possible health and care. We also use your data to:

- Confirm your identity to provide these services and those of your family / carers
- Understand your needs to provide the services that you request
- Obtain your opinion on our services
- Prevent and detect fraud and corruption in the use of public funds
- Make sure we meet our statutory obligations, including those related to diversity and equalities
- To undertake specific purposes (i.e. employing our staff, research and development etc.).
- Adhere to a legal requirement that will allow us to use or provide information (e.g. a formal Court Order or legislation)

The information in your GP health record is obtained from you and processed by staff within the GP practice (GP, nurse, administration staff) who provides direct care and administrative functions for the GP practice. The record also contains information from other sources who provide health and care services to you including:

- Hospitals
- Other GP practices
- Out of hours services
- Walk in centres
- Social care services

Explaining the legal bases we rely on to process your data

The law on data protection under the GDPR sets out a number of different reasons for which personal data can be processed for. The law states that we have to inform you what the legal basis is for processing personal data and also if we process special category of data such as health data what the condition is for processing. The types of processing we carry out in the GP practice and the legal bases and conditions we use to do this are outlined below:

Provision of Direct Care and administrative purposes

Direct care means a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. This is carried out by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship with. In addition, this also covers administrative purposes which are in the patient's reasonable expectations.

To explain this, a patient has a legitimate relationship with a GP in order for them to be treated and the GP practice staff process the data in order to keep up to date records and to send referral letters etc.

Other local administrative purposes include waiting list management, performance against national targets, activity monitoring, local clinical audit and production of datasets to submit for national collections.

This processing covers the majority of our tasks to deliver health and care services to you. In order to process your personal data for this, the legal basis under GDPR is:

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6 (1)(e) of the GDPR)

And as this is a special category of data, the condition for processing is:

Processing is 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 and social care or treatment or the management of health and social care systems and services (Article 9(2)(h) of the GDPR)

When we use the above legal basis and condition to process your data for direct care, consent under GDPR is not needed. However, we must still satisfy the common law duty of confidentiality and we rely on implied consent. For example, where a patient agrees to a referral from one healthcare professional to another and where the patient agrees this implies their consent.

Purposes other than direct care (secondary use)

This is information which is used for non-healthcare purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When your personal information is used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

Safeguarding

For the purposes of safeguarding children and vulnerable adults, the following legal basis and condition applies:

Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6 (1)(e) of the GDPR)

And,

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

Please note in the areas of safeguarding the provisions of the Children Acts 1989 and 2006 and Care Act 2014 apply and take precedent.

Processing / disclosures required by law

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

The legal basis for this is:

Processing is necessary for compliance with a legal obligation (Article 6(1)(c))

And the condition for processing is the same as above Article 9 (2)(h) as this is medical data.

Areas which fall under this remit and which the GP practice participates in are:

Type of Processing by law / statute	Details
Risk Stratification	Risk stratification entails applying computer based algorithms, or calculations to identify those patients who are most at risk from certain medical conditions and who will benefit from clinical care to help prevent or better treat their condition. To identify those patients individually from the patient community would be a lengthy and time-consuming process which would by its nature potentially not identify individuals quickly and increase the time to improve care. A GP / health professional reviews this information before a decision is made.
Invoice Validation	If you have received treatment within the NHS, the local Commissioning Support Unit (CSU) may require access to your personal information to determine which Clinical Commissioning Group is responsible for payment for the treatment or procedures you have received. Information such as your name, address, date of treatment and associated treatment code may be passed onto the CSU to enable them to process the bill. These details are held into a secure environment and kept confidential. This information is only used to validate invoices in accordance with the current Section 251 Agreement and will not be shared for any further commissioning purposes.
National clinical audit	The GP 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 data of birth and information about your health which is recorded in coded form, for example, the clinical code for diabetes or high blood pressure.
Medical Research / Health Management approved by law	The practice contributes to medical research and may send relevant information to medical research databases such as the Clinical Practice Research Datalink and QResearch when the law allows.

Purposes requiring consent

There are also other areas of processing undertaken where consent is required from you. Under GDPR, consent must be freely given, specific, you must be informed and a record must be made that you have given your consent, for example, a signature on a form or a tick in a box to confirm you have understood what you are consenting too. The legal basis and condition have the same form of words which is:

The individual has given consent to the processing of his or her personal data for one or more specified purposes (Article 6(1)(a) and Article 9(2)(a).

Areas which fall under this remit and which the GP practice participates in are:

Type of Processing with consent	Details
Subject Access Requests	The Data Protection Act and General Data Protection Regulations allows you to find out what information is held about you including information held within your medical records, either in electronic or physical format. This is known as "right of subject access". If you would like to have access to all or part of your records, you can make a request in writing. You should however be aware that some details within your health records may be exempt from disclosure, however this will in the interests of your wellbeing or to protect the identity of a third party. If you would like access to your GP record please submit your request in writing to the Practice Manager.
Text Messaging	If you provide the Practice with your mobile telephone number we may use this to send you reminders about appointments you may have at the practice or other health information and screening being carried out.
Practice Website	Our Website does use cookies to optimise your experience. My Surgery Website Limited does not set first party cookies on this website containing any personal data unless specifically instructed to do so by the user. For example, if a user requests to be remembered on a form then a cookie is set to retain this form data for next time. Using this feature means that you agree to the use of cookies as required by the EU Data Protection Directive 95/94/EC. You have the option to decline the use of cookies on your first visit to the website.

Using anonymous or coded information

Anonymous information is data that cannot be identified because as all identifiers have been removed or the data has been aggregated to a level where individuals cannot be identified.

Coded / pseudonymised information is a process that removes the NHS number and any other identifiable information such as name, date of birth or postcode, and replaces it with an artificial identifier, or pseudonym. Data which is pseudonymised is effectively anonymous to the people who receive and hold it but allows the association of multiple events with one patient, allowing us to better understand the experience of patients accessing health services.

This type of data may be used to help assess the needs of the general population and make informed decisions about the provision of future services. Information can also be used to conduct health research and development and monitor NHS performance. Where information is used for statistical purposes, stringent measures are taken to ensure individual patients cannot

be identified. Anonymous statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units and research institutions.

How we protect your personal data

We will use the information in a manner that conforms to the General Data Protection Regulations (GDPR) and Data Protection Act 2018. The information you provide will be subject to rigorous measures and procedures to make sure it can't be seen, accessed or disclosed to any inappropriate persons. We have an Information Governance Framework that explains the approach within the GP practice, our commitments and responsibilities to your privacy and cover a range of information and technology security areas.

Access to your personal confidential data is password protected on secure systems and securely locked in filing cabinet when on paper.

Our IT Services provider, Greater Manchester Shared Service regularly monitor our system for potential vulnerabilities and attacks and look to always ensure security is strengthened.

All our staff have received up to date data security and protection training. They are obliged in their employment contracts to uphold confidentiality, and may face disciplinary procedures if they do not do so. We have incident reporting and management processes in place for reporting any data breaches or incidents. We learn from such events to help prevent further issues and inform patients of breaches when required.

How long do we keep your personal data?

Whenever we collect or process your data, we will only keep it for as long as is necessary for the purpose it was collected. For a GP practice, we comply with the Records Management NHS Code of Practice which states that we keep records for 10 years after date of death. Following this time, the records are securely destroyed if stored on paper or archived for research purposes where this applies.

Who we share your data with?

As stated above, where your data is being processed for direct care this will be shared with other care providers who are providing direct care to you such as:

- NHS Trusts / Foundation Trusts
- GP's
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers

- Voluntary Sector Providers
- Ambulance Trusts
- Social Care Services
- Out of hours providers
- Walk in centres
- Clinics

We work with third parties and suppliers (data processors) to be able for us to provide a service to you. These include:

- EMIS to provide our electronic clinical system
- NHS Greater Manchester Shared service – to provide our IT services
- Shred it to destroy our confidential waste

There may be occasions whereby these organisations have potential access to your personal data, for example, if they are fixing an IT fault on the system. To protect your data, we have contracts and / or Information Sharing Agreements in place stipulating the data protection compliance they must have and re-enforce their responsibilities as a data processor to ensure you data is securely protected at all times.

We will not disclose your information to any 3rd party without your consent unless:

- there are exceptional circumstances (life or death situations)
- where the law requires information to be passed on as stated above
- required for fraud management – we may share information about fraudulent activity in our premises or systems. This may include sharing data about individuals with law enforcement bodies.
- It is required to be disclosed to the police or other enforcement, regulatory or government body for prevention and / or detection of crime

Where is your data processed?

Your data is processed with the GP surgery and by other third parties as and when required who are UK based. Your personal data is not sent outside of the UK for processing.

Where information sharing is required with a country outside of the EU you will be informed of this and we will have a relevant Information Sharing Agreement in place. We will not disclose any health information without an appropriate lawful principle, unless there are exceptional circumstances such as when the health or safety of others is at risk, where the law requires it, or to carry out a statutory functions i.e. reporting to external bodies to meet legal obligations

What are your rights over your personal data?

You have the right to request:

- Access to personal data we hold about you, free of charge (subject to exemptions) and provided to you within 1 calendar month. We request that you provide us with adequate information in writing to process your request such as full name, address, date of birth, NHS number and details of your request and documents to verify your identity so we can process the request efficiently. On processing a request, there may be occasions when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you. However, if the other person was acting in their professional capacity in caring for you, in normal circumstances they could not prevent you from having access to that information.
- The correction of personal data when incorrect, out of date or incomplete which must be acted upon within 1 calendar month of receipt of such request. Please ensure the GP practice has the correct demographic details for you.
- If we have consent for any processing we do, you have the right to withdraw that consent at any time and have the right to have data portability (a commonly used and machine readable format) and erasure (right to be 'forgotten')
- The right to object to the processing of personal data however please note if we can demonstrate compelling legitimate grounds which outweighs the interest of you then processing can continue. If we did not process any information about you and your health care if would be very difficult for us to care and treat you

To request a copy or request access to information we hold about you and / or to request information to be corrected if it is inaccurate, please contact:

The Practice Manager on 01257 421909

Postal Address: 49 High Street, Standish, Wigan, WN6 0HD

Objections to processing for secondary purposes (other than direct care)

The NHS Constitution states "You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered". The possible consequences (i.e. lack of joined up care, delay in treatment if information has to be sourced from elsewhere, medication complications which all lead to the possibility of difficulties in providing the best level of care and treatment) will be fully explained to you to allow you to make an informed decision.

If you wish to opt out of your data being processed and / or shared onwards with other organisations for purposes not related to your direct care, please contact the surgery.

There are several forms of opt- outs available at different levels. These include for example:

A. Information directly collected by the surgery:

Your choices can be exercised by withdrawing your consent for the sharing of information that identifies you, unless there is an overriding legal obligation.

B. Information not directly collected by the surgery, but collected by organisations that provide NHS services.

Type 1 opt-out

If you do not want personal confidential data information that identifies you to be shared outside your GP practice, for purposes beyond your direct care you can register a type 1 opt-out with your GP practice. This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Patients are only able to register the opt-out at their GP practice.

Records for patients who have registered a type 2 opt-out will be identified using a particular code that will be applied to your medical records that will stop your records from being shared outside of your GP Practice.

Type 2 opt-out

NHS Digital collects information from a range of places where people receive care, such as hospitals and community services.

To support those NHS constitutional rights, patients within England are able to opt out of their personal confidential data being shared by NHS Digital for purposes other than their own direct care, this is known as the 'Type 2 opt-out'

If you do not want your personal confidential information to be shared outside of NHS Digital, for purposes other than for your direct care you can register a type 2 opt-out with your GP practice.

Patients are only able to register the opt-out at their GP practice.

Complaints / Contacting the Regulator

If you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, please contact our Data Protection Officer / Practice Manager at the following contact details:

Email us at: gp-p92014@nhs.net

Or write to us at: 49 High Street, Standish, Wigan, WN6 0HD

If you are not happy with our responses and wish to take your complaint to an independent body, you have the right to lodge a complaint with the Information Commissioner's Office.

You can contact them by calling 0303 123 1133 or go online to www.ico.org.uk/concerns (opens in a new window, please note we cannot be responsible for the content of external websites)

Further Information / Contact Us

We hope that the Privacy Notice has been helpful in setting out the way we handle your personal data and your rights to control it. Should you have any questions / or would like further information, please contact either our Caldicott Guardian / Data Protection Officer / Practice Manager at the following contact details:

Email us at: gp-p92014@nhs.net

Or write to us at: 49 High Street, Standish, Wigan, WN6 0HD