**PRACTICE PRIVACY NOTICE FOR PATIENTS**

We would be grateful if you could read this notice together with any other documents we may provide when we are collecting or processing personal information about you so that you are aware of how and why we are using such information.

**The General Data Protection Regulations (GDPR)**

*Personal Data*

Personal data is data which relates to any living individual who can be identified from that data or from that data and other information such as an expression of opinion about the individual.

*What is the GDPR?*

The General Data Protection Regulation 2018 (GDPR) replaces the Data Protection Act 1998 (DPA) in governing how personal data is managed by a "controller" or "processor".

In this respect, a data controller is a person (or business) who determines the way in which, personal data is processed. A data processor is anyone who processes personal data on behalf of the data controller (not including the data controller's own employees).

A "Data Subject" is a person whose data is being processed.

Dr. O’Reilly is both the controller and processor of personal data. This means that he is responsible for deciding how we hold and use personal information about you whether you use our services directly or via a third-party.

**What is a Privacy Notice?**

A Privacy Notice (or ‘Fair Processing Notice’) is an explanation of what information the Practice collects on patients and how it is used. Being transparent and providing clear information to patients about how a Practice uses their personal data is an essential requirement of the Data Protection Act (DPA) 1998 and new General Data Protection Regulation (GDPR).

Under the DPA and GDPR, the first principle is to process personal data in a fair and lawful manner. This applies to everything that is done with patient personal information. In essence this means that the Practice must:

* have legitimate reasons for the use or collect of personal data;
* not use the data in a way that may cause adverse effects on the individuals (e.g. improper sharing of their information with 3rd parties);
* be transparent about how your data will be used and give appropriate privacy notices when collecting personal data;
* handle personal data only as reasonably expected;
* make no unlawful use of the collected data

**How Personal Data Is Collected**

Data is collected in a variety of ways:

* Direct (email, telephone, letter etc);
* The completion of a registration form, questionnaire or consent form;
* Clinical records of consultations;
* Third party information: diagnostic test results, communication from specialists etc.

**How we use your information**

This privacy notice explains why we collect information about our patients and how we use that information.

Dr. O’Reilly manages patient information in accordance with existing laws and with guidance from organisations that govern the provision of healthcare in Wales such as the Department of Health and the General Medical Council.

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

* Data Protection Act 1998
* General Data Protection Regulations 2018
* Human Rights Act 1998
* Common Law Duty of Confidentiality
* Health and Social Care Act 2012
* NHS Codes of Confidentiality and Information Security

The **Health and Social Care Act 2012** changed the way that personal confidential data is processed, therefore it is important that patients are aware of and understand these changes and that you have an opportunity to object and know how to do so.

Health records may be processed electronically on paper or a combination of both.

Records held by this GP practice may include the following information:

* Details about you such as address, telephone number and next of kin;
* Any contact the practice has had with you, including appointments (emergency or scheduled), clinic visits, etc.;
* Notes and reports about your health;
* Details about treatment and care given;
* Results of investigations, such as laboratory tests, x-rays, etc.;
* Relevant information from other health professionals, relatives or those who care for you.

The practice collects and holds this data for the sole purpose of providing healthcare services to our patients and we will ensure that the information is kept confidential. However, we can disclose personal information if:

* It is required by law
* You provide consent – either implicitly for the sake of your own care or explicitly for other purposes
* It is justified to be in the public interest

Some of this information will be held centrally and used for statistical purposes. Where we hold data centrally, we take strict and secure measures to ensure that individual patients cannot be identified.

Information may be used for clinical audit purposes to monitor the quality of service provided. Where we do this we ensure that patient records cannot be identified.

Patients can choose to withdraw their consent to their data being used.

When the practice is about to participate in any new data-sharing scheme we will make patients aware. We will also explain clearly what you have to do to ‘opt-out’ of each new scheme.

A patient can object to their personal information being shared with other health care providers but if this limits the treatment that you can receive then the doctor will explain this to you at the time.

**Mobile Telephone**

If you provide us with your mobile phone number we may use this to send you reminders about any appointments or other health screening information being carried out.

**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 the Data Protection Act 1998 (which is overseen by the Information Commissioner’s Office), General Data Protection Regulations, Human Rights Act and the Common Law Duty of Confidentiality. Every staff member has a legal obligation to maintain the confidentiality of patient information.

**Access to personal information**

You have a right under the Data Protection Act and General Data Protection Regulations to access and view information the practice holds about you, and to have it amended or removed if it is inaccurate. This is known as ‘the right of subject access’. If we do hold information about you we will:

* give you a description of it;
* tell you why we are holding it;
* tell you who it could be disclosed to;
* let you have a copy of the information in an intelligible form.

If you would like to make a ‘subject access request’, please contact the practice. You will be required to complete a subject access request form and provide ID to confirm your right to access. Under the General Data Protection Regulation there is no charge for this work and you can expect your request to be dealt with within four weeks. You will need to collect any copies of medical records in person or personally authorise a specific individual to collect on your behalf if you are not able to attend in person. You or your representative will need to provide photographic ID (or another mutually agreed form of ID if photographic ID is not available). You will also have to sign a receipt upon collection. These steps are taken to protect your data.

The practice is registered as a data controller under the Data Protection Act 1998.

**Change of Details**

It is important that you tell Dr.O’Reilly if any of your details such as your name or address have changed or if any of your details such as date of birth are incorrect in order for this to be amended. You have a responsibility to inform us of any changes so our records are accurate and up to date for you.

**Notification**

The Data Protection Act requires organisations to register a notification with the Information Commissioner to describe the purposes for which they process personal and sensitive information. This information is publicly available on the Information Commissioners Office website <https://ico.org.uk/>

**Who is the Data Controller?**

Under the Data Protection Act, the data controller is the person or organisation that will decide the purpose and the manner in which any personal data will be processed. They have overall control of the data they collect and decide how and why it will be processed.

Dr. O’Reilly is the data controller for the patient information he collects. The data controller has ultimate responsibility for compliance with the Data Protection Act.

**Suspected Breaches**

Suspected breaches on data protection can be reported directly to Dr. O’Reilly who will produce an incident report and investigate the suspected breach immediately. Serious breaches will be referred to the Information Commissioners Office.

You retain the right to report any breach directly to the ICO’s office at <https://ico.org.uk/for-organisations/report-a-breach>