Practice Privacy Statement

Risca & North Celynen Practice has a legal duty to explain how we use any personal information we collect about you, as a registered patient at the practice. Staff at this practice maintain records about your health and the treatment you receive in electronic and paper format.

What information do we collect about you?

We will collect information such as personal details, including name, address, next of kin, records of appointments, visits, telephone calls, your health records, treatment and medications, test results, X-rays, etc. and any other relevant information to enable us to deliver effective medical care.

How we will use your information

Your data is collected for the purpose of providing direct patient care; however, we can disclose this information if it is required by law, if you give consent or if it is justified in the public interest. The practice may be requested to support research;

however, we will always gain your consent before sharing your information with medical research databases when the law allows.

NHS Wales also uses relevant information about your health to help improve NHS Wales' services and public health. Information will only be used or passed on to others involved in your care if they need it. Whenever your information is used for your care, it will be handled in the strictest confidence. NHS Wales will not normally disclose your personal information without your consent, unless it is in your best interests or required by law.[1]

Processing your information in this way and obtaining your consent ensures that we comply with Articles 6(1)(c), 6(1)(e) and 9(2)(h) of the GDPR.

Maintaining confidentiality and accessing your records

We are committed to maintaining confidentiality and protecting the information we hold about you. We adhere to the General Data Protection Regulation (GDPR), the Confidentiality Code of Practice for Health and Social Care in Wales, as well as guidance issued by the Information Commissioner's Office (ICO). You have a right to access the information we hold about you, and if you would like to access this information, you will need to complete a Subject Access Request (SAR). Please ask at reception for a SAR form and you will be given further information. Furthermore, should you identify any inaccuracies, you have a right to have the inaccurate data corrected.

Risk stratification

Risk stratification is a mechanism used to identify and subsequently manage those patients deemed as being at high risk of requiring urgent or emergency care. Usually this includes patients with long-term conditions, e.g. cancer.

Invoice validation

Your information may be shared if you have received treatment to determine which local health board is responsible for paying for your treatment. This information may include your name, address and treatment date. All of this information is held securely and confidentially; it will not be used for any other purpose or shared with any third parties.

Opt-outs

You have a right to object to your information being shared. Should you wish to opt out of data collection, please contact a member of staff who will be able to explain how you can opt out and prevent the sharing of your information outside this practice.

Retention periods

In accordance with the Records Management Code of Practice for Health and Social Care 2016, your healthcare records will be retained for the duration of your life and for 10 years after your death.

What to do if you have any questions

Should you have any questions about our privacy policy or the information we hold about you, you can:
Contact the practice's data controller. GP practices are data controllers for the data they hold about their patients[2]
Write to the data controller at Risca & North Celynen Practice,
Ask to speak to the practice manager or their deputy.

Complaints

In the unlikely event that you are unhappy with any element of our data-processing methods, you have the right to lodge a complaint with the ICO. For further details, visit ico.org.uk and select 'Raising a concern'.

Changes to our privacy policy

We regularly review our privacy policy and any updates will be published on our website, in our newsletter and on posters to reflect the changes.

[1] NHS Direct Wales

General Data Protection Regulation

UK GDPR regulations apply from the 25th May 2018, and will apply even after the UK leaves the EU. What UK GDPR will mean for patients.
UK GPDR sets out key principles about processing personal data:

1. Data must be processed lawfully, fairly and transparently
2. It must be collected for specific, explicit and legitimate purposes
3. It must be limited to what is necessary for the purposes for which it is processed
4. Information must be accurate and kept up to date
5. Data must be held securely
6. It can only be retained for as long as is necessary for the reasons it was collected

There are also stronger rights for patients regarding the information that Practices hold about them. These include:

1. Being informed about how their data is used
2. Having access to their own data
3. Ask to have incorrect information changed
4. Restrict how their data is used
5. Move their patient data from one health organisation to another
6. The right to object to their patient information being processed (in certain circumstances).
7.

What is UK GDPR

UK GDPR stands for General Data Protection Regulation and is a piece of legislation introduced in May 2018 along with the Data Protection Act 2018, sets the regulation about how organisations must handle information in the UK. UK GDPR applies to the UK and EU; it covers anywhere in the world in which data about EU citizens is processed.
UK GDPR has strengthened many of the principles of the previous UK legalisation known as the Data Protection Act 1998. The main changes are:

- Practices must comply with subject access requests within one calendar month
- Where we need your consent to process data, this consent must be freely given, specific, informed and unambiguous
- There are new, special protections for patient data
- The Information Commissioner's Office must be notified within 72 hours of a data breach
- Higher fines for data breaches

What is consent?

Consent is permission from a patient – an individual's consent is defined as "any freely given specific and informed indication of a patient's wishes by which the data subject signifies their agreement to personal data relating to them being processed."

To protect your right to privacy, and we may ask you to provide consent to do certain things, for example completing a medical report. Individuals also have the right to withdraw their consent at any time.