PRIVACY POLICY FOR THE DENTAL ACCESS PORTAL

WHY WE USE PERSONAL DATA

The Dental Access Portal provides a central platform for Health Boards to allocate places for routine dental treatment at NHS dental practices across Wales. The new service has been designed, built and hosted by Digital Health and Care Wales (DHCW) and hosted on a Microsoft Power Platform.

Patients provide information to enable their details to be added to the Dental Access Portal. The Dental Access Portal is then used to allocate places for routine dental treatment where spaces become available. A registered person will be able to authenticate to the external site and access their registered details to make amendments or remove themselves from the Dental Access Portal.

Access to the Dental Access Portal is controlled. Only those users with a legitimate reason to access this information (such as to allocate you a dental practice, update your information or for maintenance of the system) will be able to access this information. Access to personal data is only undertaken where it is required for somebody to do their job. Confidentiality and privacy of information is taken seriously and all employees accessing this information are required to be trained on the appropriate use of personal data. Inappropriate access to personal data can result in disciplinary action, including dismissal.

TYPES OF PERSONAL DATA

To register members of the public's details on the Dental Access Portal, we collect, store and use a range of personal data ('processing').

We do not collect or process all of this personal data about all patients all of the time. We only collect and process the personal data necessary for the particular task that we are carrying out. Where possible, information about you will be pseudonymised (replacing identifiers with codes or 'keys') or anonymised (meaning individuals cannot be identified); for example when reports are produced.

The personal data we process includes:

- Full name
- Date of Birth
- NHS Number
- Address
- Contact details such as email address, mobile phone or landline
- Communication language and preferred treatment languages
- Whether you have any special requirements for the purposes of allocating you a dentist that is able to meet these requirements
- The above personal data, where you care for another person

HOW WE USE PERSONAL DATA

Personal data is collected in order for Health Boards to fairly and accurately allocate available NHS dental practice spaces to individuals based on their clinical need, personal requirements and the period of time they have been waiting for NHS dental care.

DHCW shall assume a Controllership responsibility for the data processed within the Data Access Portal, will liaise with Welsh Government, Health Boards, and other appropriate NHS Wales statutory bodies when in consideration of use of the data for the other purposes of processing, dissemination and matters in relation to the use and performance of the system.

HOW WE OBTAIN PERSONAL DATA

Data will be obtained from patients submitting their information as part of their registration to the Dental Access Portal, either directly, via proxy access (such as on behalf of another person) or via a Health Board administrator.

Data will also be obtained from existing waiting lists for NHS dental services owned by Health Boards, which will be uploaded to the new system. Patients whose information is uploaded from an existing list will have the opportunity to amend this information and ask to be removed from the Dental Access Portal.

THE LAWFUL BASIS FOR WHAT WE DO

Data protection legislation requires us to tell you the lawful basis for processing personal data in the way we do. Further information is available from the website of the Information Commissioner's Office. Click here for more information.

For the purposes of allocating places for routine dental treatment at NHS dental practices across Wales, we generally rely on the following legal provisions:

- Public task: the processing is necessary to perform a task in the public interest.
- The provision of care: the processing is required for the purposes of health or social care or treatment or the management of health or social care systems.

DHCW have been directed by Welsh Government to undertake work to introduce the Dental Access Portal within primary care in Wales, which will enable Health Boards to allocate patients based on need to appropriate dental practices. Together, alongside DHCW's statutory functions provides DHCW with the authority to collect relevant data for this purpose. For further information about our DHCW's establishment and functions, please see: Digital Health and Care Wales: establishment and functions | GOV.WALES

WHO PERSONAL DATA IS SHARED WITH

Personal data is only shared with other organisations where it is necessary and lawful to do so.

Information will be shared with:

- Digital Health and Care Wales - DHCW is a Special Health Authority, part of the NHS Wales family and a trusted partner. DHCW design, built and host the Dental Access Portal.
- Welsh Health Boards – as users of the Dental Access Portal, limited Health Board administrators will have access to the system to manage and allocate places for routine dental treatment at NHS dental practices across Wales.
- Welsh Dental Practices – Welsh Dental Practice employees will receive information via the Welsh Health Board on patients who have been accepted a placement. Welsh Dental Practice employees will not have access to the Dental Access Portal and will only see the personal data of those patients that have accepted the allocation.

The solution uses GOV.notify to send automated communications to patients. These messages are initiated by the Health Board administrator within the Dental Access Portal. Only relevant information will be shared with Gov.Notify Service for the purposes of sending communications to the patient. Patients will only be communicated for the purposes of allocating places for routine dental treatment at NHS dental practices in Wales.

The solution hosted on a Microsoft Power Platform with information stored in the UK. Information submitted to the Gov.UK Notify service is stored on the secure Gov.UK infrastructure in the UK.

Anyone receiving personal data about you is under a legal duty to keep it confidential. We only request, use and share the minimum personal data necessary. We will never sell personal data about you and we will not share it without the appropriate legal authority, or if appropriate to the circumstances, your informed consent.

We may share personal data for other purposes; for example, to allow research to take place where it is in the public interest. This is subject to an approval process. Service planning or commissioning, and audit are some other purposes that may require personal data to be shared. Anonymised or pseudonymised data will be used where possible and uses of personal data are subject to approval processes.

We will share personal data if we are required to do so by law – for example, by court order or to prevent fraud or other crimes.

HOW LONG WE KEEP PERSONAL DATA

We keep personal data for as long as we need to in order to fulfil the purposes for which it was collected, in line with the Records Management Code of Practice for Health and Social Care and to comply with our legal and regulatory obligations.

Information within the Dental Access Portal will be retained for 7 years to ensure that information is kept in the event of audit, investigation and liability claims.

SECURITY AND STORAGE OF DATA

We recognise that personal data is very valuable and so we take its security very seriously. The Dental Access Portal system has processes in place to prevent unauthorised access or disclosure of data through the use of:

- Auditing - we keep records of those who access personal data;
- Access controls - members of staff are provided with their own username and password to access personal data;
- Electronic records management - all records are stored confidentially and in secure locations;
- Computer controls - We have complex security controls to ensure our computers cannot be accessed

by those not authorised to do so – such as hackers; and

- Encryption - computer devices that hold personal data such as laptops are encrypted in case the device storing the data is lost or stolen

All staff accessing the Dental Access Portal must complete Information Governance training. This training makes staff aware of the importance of the confidentiality and security of personal data and makes clear that they are personally responsible for the security of such data. This training must be completed every two years.

We also make sure that any third parties we deal with keep all personal data they process on our behalf safe and secure.

YOUR RIGHTS

Data Protection legislation provides various individual rights for data subjects including:

- Right to be informed
- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Not all of these rights are absolute, which means we often have to balance your wishes against other requirements. For example, if you have been allocated a dentist, it is unlikely that a request from a data subject to delete a record of this would be agreed.

This is because there are other legal reasons that such records need to be kept. We need to retain this information to ensure that we have accurate logs of who may have been allocated. Each request to exercise one of the above rights will be assessed on its merits.

For an explanation of all your rights please see the ICO's guidance, which you can access here.

If you wish to exercise any of these rights or have any queries or concerns regarding our processing of personal data about you, please use the contact details provided below, who will be able to direct you to the relevant organisation.

CHANGES TO THIS POLICY

We keep our privacy policy under regular review to ensure it remains relevant, accurate and up to date. Any changes to this privacy policy will apply to you and the information held about you immediately.

CONTACT US

Please contact DHCW's Data Protection Officer for further information regarding this policy, including how to exercise your rights: Data Protection Officer

Digital Health and Care Wales

Tŷ Glan-yr-Afon

21 Cowbridge Road East

Cardiff

CF11 9AD

DHCW.InformationGovernance@wales.nhs.uk

RIGHT OF COMPLAINT

You have the right to lodge a complaint in relation to this privacy notice or our processing activities with the Information Commissioner's Office, which you can do through the website or their telephone helpline.

https://ico.org.uk/global/contact-us/

DEFINITIONS

Data Protection Officer - Certain categories of organisation, including any public body or authority (except courts in their judicial capacity) are required to designate a suitably qualified Data Protection Officer (DPO). The tasks of the DPO are set out in Article 39 of
UK GDPR

Data subject - A 'data subject' is an identified or identifiable natural person.

Data Protection Legislation - The UK GDPR is the retained EU law version of the EU's General Data Protection Regulation (GDPR). It contains the definitions, conditions, principles and rights that apply to the processing of personal data in the UK.

The Data Protection Act 2018 creates specific provisions, such as exemptions allowed by UK GDPR, and incorporates the provisions of EU Data Protection Directive 2016/680 – the Law Enforcement Directive.

Personal data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Processing - Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Profiling - Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

Pseudonymised data / Pseudonymisation
- The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Version 1.0 – last updated 07/06/24