



IGDC • DHCW



GIG
CYMRU
NHS
WALES

Iechyd a Gofal
Digidol Cymru
Digital Health
and Care Wales

Privacy Notice



HOW DIGITAL HEALTH AND CARE WALES HANDLES DATA ABOUT YOU

WHY WE USE PERSONAL DATA

The personal data we hold reflects the varied nature of our role. Below are some examples of DHCW activities:

- We host and maintain national IT systems used to provide care to the people of Wales;
- We develop and test new systems;
- We work on behalf of Health Boards and other organisations in Wales to link IT systems to ensure that doctors, nurses and other health and care professionals have the information they need to provide care to the people of Wales;
- We provide services that set information standards, making sure that IT systems use a common language; and
- We analyse information to provide reports and inform priorities for the NHS in Wales.
- We provide reports to NHS Wales organisations to assist with various activities such as management of resources, clinical audit, improvement planning. For more information, please visit DHCW website at www.dhcw.nhs.wales

All of the above activities require access to personal data. This access is controlled – not all of the people working for us need access to all the personal data we hold, and we only allow access to personal data where it is required for an individual to do their job. Digital Health and Care Wales (DHCW) take this seriously and all of our employees are required to be trained on the appropriate use of personal data. Inappropriate access to personal data can result in disciplinary action, including dismissal.

For further information about our DHCW's establishment and functions, please see: Digital Health and Care Wales: <https://www.gov.wales/digital-health-and-care-wales-establishment-and-functions>



TYPES OF PERSONAL DATA

To fulfil our functions and provide services, we collect, store and use a range of personal data ('processing'). We do not collect or process all of this personal data about all people 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 categories of personal data we process include:

- Contact details, including names, aliases, addresses, postcodes, telephone numbers and email addresses;
- Identifying details, including date of birth and reference numbers such as NHS numbers;
- Information about people's health and wellbeing including medical history, potentially including genetic data;
- Workplace, education or financial information;
- Information about patients' family, dependents or personal circumstances (to ensure professionals know who they can speak to about their care);
- Other information that could impact on the way people are treated or cared for, or which we are required to collect to understand who is

using health and care systems. This includes data about people's religion, race, ethnicity, gender and sexual orientation;

- Online identifiers, including IP addresses and cookie identifiers (collected when you visit websites DHCW are responsible for).
- Information regarding NHS Wales workforce for purposes such as account maintenance, training etc.

HOW WE USE PERSONAL DATA

In the main, we process personal data for purposes directly connected with ensuring that we support clinical professionals, helping them provide high quality health care to patients in hospitals, GP practices and across the community. However, we also process it for other general reasons, such as:

- Providing you with information you have requested;
- Handling your enquiries, complaints or concerns;
- Providing access to certain areas of our websites;
- Informing you of services which may be relevant to you;
- Taking part in processing data for clinical audit to ensure safety of patient;
- Using information in the context of your age, sex and other factors to offer, for example, screening services or immunisations. Such services are usually offered by other organisations, but we often hold



the information and facilitate the analysis;

- Taking part in research to help assess new treatments, technologies or methods and help better understand health and specific conditions;
- Auditing and improving our IT systems and websites;
- Facilitating stakeholder engagement such as focus groups or surveys;
- Providing information to regulatory bodies; and
- Sharing personal data to resolve complaint or to obtain legal advice or in relation to a claim.

DHCW may use artificial intelligence (AI) to fulfil our functions.

Some examples include:

- Generating pre-read material in preparation for meetings.
- Summarising lengthy documents, emails or when used during meetings to summarise the meeting so far.
- Post-meeting to produce meeting notes or minutes, and to provide a summary of the meeting to staff who were not able to attend.
- Text and other content generation. For example, to produce the first draft of an email, briefing paper or presentation.
- Tips regarding troubleshooting, coding or external product use

Human oversight is always required to verify outputs.

HOW WE OBTAIN PERSONAL DATA

We collect personal data from a variety of sources, including (but not limited to):

- Information provided by other NHS organisations (e.g. Health Boards, Trusts and GPs);
- Information provided by non NHS organisations (e.g. Local Authorities);
- Other sources of UK wide information (e.g. NHS Digital and Office of National Statistics);
- Surveys and research commissioned by us or other organisations; and
- Information you provide directly to us.

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. [Click here for more information.](#)

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.

Where we deem appropriate, we may ask permission to use personal data about you.

WHO PERSONAL DATA SHARED WITH

Personal data is only shared with other organisations where it is necessary and lawful to do so. The range of information sharing partners reflects the wide scope of services and systems we are involved with. Our information sharing partners include:

- NHS organisations in Wales such as Health Boards, General Medical Practices and Pharmacies;
- Other care providing organisations, such as Local Authorities; and
- Suppliers of IT systems, some of whom are private companies who provide services under contract.

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.

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 and the implementation of appropriate controls.

HOW LONG WE KEEP PERSONAL DATA

We keep personal data for as long as we need to in order to fulfil the purpose(s) for which it was collected and to comply with our legal and regulatory obligations. NHS Wales has records retention schedules that identify the minimum term data should be kept.

This is available via the Welsh Government website available [here](#).

SECURITY AND STORAGE OF DATA

DHCW recognises that personal data is very valuable and so we take its security very seriously. We have set up systems and processes to prevent unauthorised access or disclosure of data through the use of:

Auditing - we keep records of those who access personal data;

- Password controls - members of staff are provided with their own username and password to access personal data;



- Access controls – only those staff that are required to access the data have access to the data;
- Electronic records management - all healthcare 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;
- Storage – We have sophisticated storage solutions with back up for resiliency; 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 DHCW staff 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. DHCW used various methods of storage for personal data including:

- Data managed and stored by DHCW using cloud services
- Data managed and stored by DHCW within Wales
- Data managed and stored by contracted 3rd parties

Personal data may be stored outside of the European Economic Area. If this occurs, we are obliged to have in place appropriate safeguards implemented with a view to protecting data in accordance with applicable laws. Please use the contact details below if you want more information about the safeguards that are currently in place.



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, it is unlikely that a request from a data subject to delete their entire health record would be agreed. This is because there are other legal reasons that such records need to be kept.

If future treatment is required, the individual could be at risk of harm if information about their medical history is not available. Each request to exercise one of the above rights will be assessed on its merits. Some rights are unlikely to apply in the context of the work we do; for example, the right to erasure and the right to data portability.

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 contact us using the contact details provided below.

OUR WEBSITES

GOOGLE ANALYTICS

Our websites may use Google Analytics (external website), a web analytics service provided by Google Inc. ('Google'). Google Analytics uses 'cookies' and JavaScript code to help analyse user activity on websites. The information generated about your use of the website (including your IP address) will be transmitted to and stored on Google servers in the United States.

Google will use this information to produce user activity reports for the website visited. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf.



Google will not associate your IP address with any other data previously held. You may refuse the use of cookies by selecting the appropriate settings on your browser. Please note that if cookies are disabled, you may not be able to use the full functionality of this website.

By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

Read [Google's Full Privacy Policy](#) (external website) and [Terms of Service](#) (external website) for detailed information.

WHAT ARE COOKIES?

Cookies are small files that websites put on your computer hard disk drive when you visit. Cookies pass information back to websites each time you visit. They are used to uniquely identify web browsers, track user trends and store information about user preferences. You can restrict/disable cookies on your browser; please note that some website features may not function properly without cookies.

SEARCH ENGINE

Our website may contain search facilities. Search queries and results may be logged anonymously to help us improve our website and search functionality. No identifiable personal data will be collected by us.

PURPOSE AND LEGAL BASIS FOR PROCESSING

The purpose for implementing all of the above is to maintain and monitor the performance of our websites and to constantly aim to improve the sites and the services it offers to our users.

LINKS TO OTHER WEBSITES

Our websites and websites hosted by us may contain links to other websites. This policy only applies to DHCW and does not cover other organisations websites. These organisations should have their own terms and conditions.

CCTV

Our offices may have CCTV cameras and if you visit us in person you may be recorded. Any office that has CCTV cameras will have clear signs to indicate the presence of the cameras. These cameras are for security purposes, and the video will not be used for any other purpose.

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 the Data Protection Officer for further information regarding this notice, including how to exercise your rights or if you wish to make a data protection complaint:

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

If, after receiving our response, you remain dissatisfied, you have the right to complain to the Information Commissioner's Office (ICO), which you can do through the website or their telephone helpline.

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





DEFINITION

Term	Definition
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 data protection regime is set out in the Data Protection Act 2018, along with the UK General Data Protection Regulation (UK GDPR).
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.
Personal information	Includes information falling within the definition of 'personal data' and information about deceased individuals. Data protection legislation does not apply to information about deceased individuals but such information needs to be treated confidentially.
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 information / 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.