Welsh Control Standard for electronic health and care records

Providing assurance and common standards to the systems which support shared electronic health and care records

Version No. 5.0
Status: Final

Author: Siân Howson, DHCW
Approver: Darren Lloyd, DHCW

Date: 04/08/2025
Next Review Date:04/08/2027

Digital Health and Care Wales Headquarters
Tŷ Glan-yr-Afon
21 Cowbridge Road East
Cardiff
CF11 9AD
https://dhcw.nhs.wales/

Document History

Welsh Control Standard for electronic health and care records

Revision History

Date	Version	Author	Revision Summary
03.04.17	V1.0	S Howson / A Fletcher	Final Version
23.05.17	V2.0	J Short /	Review of structure and refinement of sections following feedback. Incorporation of Medical Director comments.
22.06.17	V2.1	R Wheeldon	Changed name of Register of Information Sharing Systems
16.12.19	V2.2	Andrew Fletcher (IGMAG Policy Sub Group)	Review of control standard text, review of structure, refinement of sections, updates to references in line with GDPR
03/01/20	V3.0	Andrew Fletcher (IGMAG Policy Sub Group)	Final
22/02/22	V3.1	Marcus Sandberg / Andrew Fletcher	Review
13/04/2022	V4.0	Marcus Sandberg	Final
11/03/2025	V4.2	Siân Howson	Review of control standard text, minor changes to bring up to date.
02.06.2025	V4.3	Siân Howson	Further review of text, scope and references including to reflect the DUAA
04.08.2025	V5.0	Siân Howson	Final

Authorisation

Signing of this document indicates acceptance of its contents

Author's Name: Siân Howson
Role: Senior Information Governance Officer, Digital Health and Care Wales
Recoverable Signature X Signed by: Sian Howson (Si097653)

Approver's Name: Darren Lloyd
Role: Associate Director for Information Governance and Patient Safety, Digital Health and Care Wales
Recoverable Signature X D. Lloyd Signed by: Darren Lloyd (da080063)

Contents

Section 1: Introduction 5
Section 2: Purpose 5
Section 3: Obligations 6
Section 4: Example Mechanisms for the Sharing of Personal Data 7
4.1 Data Protection 7
4.2 Common law duty of confidentiality 7
Section 5: Privacy by Design 8
Section 6: Access and Appropriate Use 8
6.1 Authorising access permissions 8
6.2 Terms of access to shared electronic health records 8
6.3 Role based access 8
6.4 Authentication of users 9
6.5 Registration and removal of user access 9
6.6 Authorising and managing workforce access 10
6.7 Environmental Security – timeouts 10
Section 7: Individual Rights 10
7.1 Key principles and messages 10
7.2 Individual Rights Requests (including Subject Access Requests) 10
7.3 Data Quality 11
7.4 Inaccurate information derived from the Welsh GP record (WGPR) 11
Section 8: Auditing and Assurance 12
8.1 Management of National Intelligent Integrated Audit Solution (NIIAS) notifications 12
8.2 Information Governance Toolkit 12
Section 9: Records Management 13
Section 10: Business Continuity 13
Section 11: Policy, Incident and Complaint Management 13
11.1 Policies, procedures and the reporting of incidents 13
11.2 Complaints and Incidents 14
Section 12: Service Portfolio 14
Section 13: Signup 14

Welsh Control Standard for electronic health and care records

Section 1: Introduction

Health and social care organisations are developing closer links to deliver a strategic vision for transforming health and wellbeing services to the people of Wales. Delivering this prudent health and integrated care vision relies on improved, secure access to electronic health and care records that are focussed on the individual; not the disease, service or organisation where the care is being delivered.

Incremental progress is being made through a mixture of systems, software and national databases which make parts of the record available in different care settings. In reality, the complete record is likely to continue to be a combination of electronic and paper held in multiple organisations. This mixed landscape is likely to cover, but not be limited to:

- One organisation allowing another access to their healthcare systems. For example, GPs having access to a secondary care system;
- Multiple organisations contributing to a shared database. For example, the Welsh Results Reporting Service (WRRS) and Welsh Care Records Service (WCRS).

A *Welsh Control Standard for Electronic Health and Care Records ('Control Standard')* webpage is available on the NHS Wales Information Governance website to provide further support and guidance for organisations on implementing the Control Standard. All Health Boards and NHS Trusts in Wales must sign the Control standard in order to use national systems. Other organisations, such as primary care contractors (e.g. GMPs) who require access to national systems must also sign the Control Standard.

Formal adoption of the Control Standard is the responsibility of an organisation's Chief Executive or Chief Officer.

On signing the declaration, each organisation agrees to support the adoption, dissemination and implementation of the Control Standard. The signatory should have overall responsibility for service user information within their organisation, for example the Senior Information Risk Officer (SIRO), Caldicott Guardian or person with similar seniority.

Section 2: Purpose

This document, the Control Standard, describes the assurances and common standards that apply to the systems which support shared electronic health and care records in Wales and provides the mechanism through which organisations commit to them.

The Control Standard provides reassurance that appropriate information governance and security measures are in place across Wales. It outlines a consistent approach for the appropriate access and use of electronic health and care records. The Control Standard also shows an ongoing commitment to collaborate to address data protection challenges, develop and implement standards and foster a culture of transparency and accountability to provide a unified consistent approach to data governance.

Each organisation will ensure that:

- Processing will be conducted within the legal framework of the UK General Data Protection Regulation (UK GDPR) (Regulation (EU) 2016/679), the Data Protection Act 2018 (DPA), the Data (Use and Access) Act (2025), the Human Rights Act 1998, in compliance with the common law duty of confidence and any other relevant legislation.
- It will only share information where it has the legal authority to do so and that there are no statutory or other legal restrictions which prevent the sharing from taking place.

  See Appendix 1 – A for further information.

Section 3: Obligations

All personal information will be processed in accordance with Data Protection legislation, the common law duty of confidence and other relevant legislation. For the purpose of this document, the term 'Service User' information' will include 'personal data' or 'special category data' as defined by data protection legislation.

Each organisation will show their agreement in working towards this Control Standard by:

- Ensuring that the commitments under the Control Standard are implemented and monitored via appropriate policies and procedures.
- Implementing robust information governance processes and data quality standards to protect the service user and other organisations from unnecessary exposure to risk.
- Agreeing that Service User information accessed through a shared record environment, will only be used by a service user for the execution of their duties.
- Being open and transparent, making best, appropriate and proportionate efforts to inform service users of how their information is used and who it will be shared with.
- Appropriately managing, controlling, monitoring and auditing Service User information limiting access to those that have a legitimate, or professional need to ensure that service user information is protected and can be shared with confidence.
- Informing the relevant parties (i.e. other NHS Organisations, Welsh Government, Information Commissioners Office) when a breach of confidentiality is identified
- Ensuring that the staff responsibilities set out in Appendix 1 - C are upheld.
- Committing to providing all relevant staff regular training in information governance, the use of information and the related information systems and applications;
- Using existing employment, legal and professional standards and processes to determine appropriate sanctions where misuse of Service User information has been identified
- Committing to continuing to review and refine our data protection policies and procedures to ensure they remain aligned with evolving legal requirements and best practices.
- Signing the 'Declaration of Acceptance and Participation' provided via an online form.

Section 4: Example Mechanisms for the Sharing of Personal Data

4.1 Data Protection

For the purposes of this Control Standard, the following conditions from the UK GDPR will usually be relied upon (legal basis for specific services will be set out in the Service Portfolio):

Article 6(1)(a)(c) and (e):

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

(c) processing is necessary for compliance with a legal obligation;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 9(2)(a)(h) and (i):

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

(h) processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member state law or contract with a health professional.

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

See Appendix 1 - B for further information.

4.2 Common law duty of confidentiality

Obligations under the common law duty of confidence must be considered alongside those of the UK GDPR and other relevant legislation. Information used for direct care purposes relies on the principle of implied consent.

Section 5: Privacy by Design

Organisations have the responsibility for ensuring Data Protection Impact Assessments (DPIAs) have been fully considered in line with UK GDPR Articles 35 and 36 and sharing these across organisations or services for transparency and scrutiny, where required. This will be of particular note, where local DPIAs are produced which involve linking to national systems or access. A similar process should be in place for Cloud Risk Assessments. It is recognised that DPIAs and Cloud Risk Assessments may be complex or simple by nature, that this should be proportional to the project or change and reflect the associated risk.

Section 6: Access and Appropriate Use

6.1 Authorising access permissions

Access to shared records will continue to be authorised at a local level following local procedures on the basis of there being a legitimate purpose.

Staff must be mindful of their responsibilities when processing service user information, and must remain compliant with mandatory information governance training.

See Appendix 1 - C for further information.

6.2 Terms of access to shared electronic health records

Access to any shared electronic record must only be obtained where:

- Accounts are linked to an individual;
- There is a legitimate purpose for access;
- They only access information relevant to their job role.

Access to service users' health records is logged and audited in compliance with UK Laws, Codes of Practice and rigorous NHS Wales requirements.

Further supplementary information on this section can be found in Appendix 1 - D.

6.3 Role based access

Role based access is an approach to restricting system access to authorised users. Where systems and applications have role based access controls, controllers are responsible for following the agreed account management processes and procedures.

Account Control 3 (AC3) is a role based access control mechanism for a number of services including the Welsh Demographic System. A fundamental principle of AC3 is that organisations manage their own users access. This requires a hierarchy to be established and maintained. The hierarchy is managed through a

‘workgroup’ structure, with specific functionality (including permissions to authorise users) associated with each workgroup. Each organisation must manage a AC3 hierarchy which allows for the approval, rejection and management of workgroups, including appointing an appropriate user in the most senior AC3 user at each organisation (known as the “Caldicott Guardian” workgroup).

Users responsible for managing other users access (such as the users in the Caldicott Guardian, Caldicott Delegate or Service Delegate workgroups) must have ensure they:

- Allocate roles where there is a legitimate use;
- Verify the identity of the user;
- Identify the reasons which justify giving access;
- Assign an appropriate level of access, relevant to the user’s use;
- Remove user access where no longer required.

For further information see Appendix 1 - E.

6.4 Authentication of users

Access to NHS Wales wide systems must be controlled by use of unique log on credentials for system users in order for them to always be uniquely identified. The NHS Wales-wide NADEX credentials must be used barring exceptional circumstances.

Local processes must ensure that system users are aware that they must log on to the system using their own credentials and do not share user credentials and passwords.

6.5 Registration and removal of user access

Standard procedures and documentation must be developed as part of the user access registration and removal process. Each organisation must have a robust system for the management of user registration processes, in particular new starters, movers and leavers. Where staff no longer have a legitimate right to access the system, access must be removed immediately.

Registering users must consist of the following requirements as a minimum:

- Identity must be verified;
- A correctly completed user request form (or suitable alternative) must be completed and appropriately authorised prior to access being granted or terminated; and
- All user registration details must be periodically reviewed to ensure that they are accurate and that access is still required.

For further information see Appendix 1 – F.

6.6 Authorising and managing workforce access

Access must be provided and managed at local level and on the authority of the employing organisation. Organisations must only grant access after ensuring that the appropriate safeguards are written into the contract or agreement. Staff must complete an appropriate level of information governance training before access is allowed. This applies to the workforce of NHS Wales organisations including staff, students, trainees, secondees, volunteers, contracted third parties and any other persons undertaking duties on behalf of NHS Wales.

6.7 Environmental Security – timeouts

Unattended workstations must be protected against unauthorised use with a short span automatic timeout facility. The onus remains with the user to maintain patient confidentiality, and the need to log-out after using the facility must be emphasised during user application training.

Section 7: Individual Rights

7.1 Key principles and messages

Service users have a right to be informed of how their information is used. The concept of transparency is an important part of data protection legislation and organisations should ensure they meet the relevant requirements. Organisations will communicate with service users through various methods to reach as wide an audience as possible. Examples include:

- Privacy information;
- Posters, leaflets and other printed materials;
- Press releases;
- News events - campaign launches, interviews;
- Social Media;
- Websites.

These messages will include how the organisation uses service user information and the benefits of sharing information.

7.2 Individual Rights Requests (including Subject Access Requests)

Each organisation must have in place policies and procedures that will facilitate the effective processing of individual rights (including Subject Access).

The UK GDPR provides the following rights for individuals:

- The right to be informed;
- The right of access;

- The right to rectification;
- The right to erasure;
- The right to restrict processing;
- The right to data portability;
- The right to object;
- Rights in relation to automated decision making and profiling.

Any individual right requests received must be processed as soon as possible and at least within the timescales expressed by data protection legislation, taking into account the prompt but reasonable time needed to review the information where appropriate.
Where more than one organisation has contributed information to a shared record then the lead organisation (i.e. the organisation receiving the request) will:

- Have responsibility for processing the request;
- Will process the request within the legislative timescale;
- If appropriate and practicable in terms of the scope and volume of the request, consult with other organisations that have contributed to the shared record

It is not always possible to consult with all Controllers if the information is made available in systems that bring together individual contributions and silo of data from other organisations. Therefore, the receiving Controller should have the disclosure responsibility on all the information made available to them.

7.3 Data Quality

Organisations must have local policies and procedures in place for the processing of service user information and for checking the accuracy of that information.

Checks on the accuracy of service user information must occur whenever the service user contacts the service. Further information and examples can be found in Appendix 1 - G.

Organisations must ensure, where possible, that systems used to share information will connect to the national demographic reference systems; the Welsh Demographic Service (WDS) and the Master Patient Index (MPI), to ensure service users are correctly identified, NHS numbers are accurate and demographic data is synchronised. See Appendix 1 – H for further information on the Master Patient Index.

7.4 Inaccurate information derived from the Welsh GP record (WGPR)

The GP record is considered to be the core health record of a patient. It is also a vital link to investigations of alleged incidents and complaints.

The WGPR is derived from the GP record and therefore, if any inaccuracies are identified in the WGPR this must be reported to the relevant GP practice as these can only be corrected on the GP clinical system.

Section 8: Auditing and Assurance

Auditing of user access is essential in order to assure that those with access to service user data have not abused the trust invested in them. Auditing activity may take place through a variety of methods, the most appropriate of which will be determined by the circumstances of the individual system.

8.1 Management of National Intelligent Integrated Audit Solution (NIIAS) notifications

The National Intelligent Integrated Auditing Solution (NIIAS) has been procured to proactively audit national shared electronic health record systems. All organisations must have local policies and procedures in place for managing NIIAS notifications. For further information on NIIAS see the supplementary information and guidance in Appendix 1 – I.

Each organisation must make local decisions on how potential incidents identified when auditing are reviewed. The review should distinguish between actual misuse and accesses which are legitimate. As a minimum, the local procedure must contain the following:

- A local communication approach with information on appropriate and inappropriate conduct and subsequent actions arising from findings of misuse;
- Detail on how incidents of potential misuse will be pursued with detail of how each outcome will be actioned;
- Guidance to support line managers, including scenarios of typical misuse, follow up action and likelihood of disciplinary action. This should be in line with local predetermined approaches developed with local Workforce & Organisation Development teams or equivalent.

This list is not exhaustive and can be added to in line with organisational policies and procedures.

8.2 Information Governance Toolkit

The Welsh Information Governance Toolkit (WIGTK) is a self-assessment tool enabling organisations to measure their level of compliance against national Information Governance standards and legislation. The assessment will help identify those areas which require improvement and assist in informing organisations' information governance improvement plans.

The WIGTK has been developed over a number of years, covering a broad range of Information Governance topics. The WIGTK requirements are split into two levels of assurance, the first level is required to obtain good compliance and assurance against national Information Governance standards and legislation. The second level can only be achieved when the first level has been attained. The second section is not mandatory and is up to the organisation whether they wish to partake in this section. The two levels are noted below:

- Minimum Expectations
- Expectations Exceeded

The WIGTK will automatically generate an achievement status on the basis of the Organisation's self-assessment, these are:

- Minimum Expectations Not Met (Non-compliant position)

- Minimum expectations Met (Compliant position)
- Expectations Exceeded X% (Compliant position)

The question sets are based on the ICO's accountability framework and are developed for NHS Wales Organisations. The WIGTK runs in conjunction with the financial year and organisations are required to submit their form on an annual basis and are expected to meet the compliant position of Minimum Expectations Met or above. This will enable organisations to demonstrate they can be trusted to maintain the confidentiality and security of both personal and business information. This will provide reassurance to staff, patients and service users that their information is processed securely and appropriately, while providing confidence to other organisations where sharing is made, that appropriate information governance arrangements are in place.

Section 9: Records Management

Organisations must have local policies in place setting out the organisations approach to records management of corporate and health records, which must align with the Records Management Code of Practice for Health and Social Care 2022.

For further information see Appendix 1 - J.

Section 10: Business Continuity

Organisations are required to have local business continuity processes in place in the event of unforeseen circumstances which would otherwise compromise that availability of national shared electronic health records.

Section 11: Policy, Incident and Complaint Management

11.1 Policies, procedures and the reporting of incidents

The Board (or equivalent) within each organisation has overall responsibility for Information Governance compliance. The Board must ensure that:

- The provisions within this Control Standard are adopted;
- All procedures required to comply with this Control Standard are created and implemented;
- Nationally agreed policies and procedures, agreed at the Information Governance Management Advisory Group are implemented within their organisation;
- Robust incident/event reporting procedures are in place.

For further information see Appendix 1 – K.

11.2 Complaints and Incidents

Each organisation will have a formal procedure by which service users, organisations and practitioners subject to this Control Standard can direct any complaints regarding the sharing of health records as described in this standard.

Organisations should ensure they work collaboratively when notified of a complaint or incident that may effect or span across organisations or services. Where necessary, organisations should work together to undertake any investigations.

For further information see Appendix 1 - K.

Section 12: Service Portfolio

The Service Portfolio sets out the core national systems that hold shared electronic health and care records. The portfolio is maintained by Digital Health and Care Wales. The systems documented in the Service Portfolio are subject to the principles outlined in the Control Standard.

The Service Portfolio information provides clarity to organisations that each sharing arrangement meets the nationally agreed standards. Inclusion of a system in the Service Portfolio or the signing up to the Control Standard does not mean that all organisations will gain automatic access to that system.

Section 13: Signup

A list of organisations who have signed up to the control standard will be maintained by Digital Health and Care Wales and may be made available on request. Details regarding how to sign up are available via the NHS Wales website.