Welsh Control Standard for electronic health and care records

Appendices - supplementary to the Control Standard

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

Revision History

Date	Version	Author	Revision Summary
03.04.17	V1	S Howson / A Fletcher	Final Version
23.05.17	V2	J Short	Review of structure and refinement of sections following feedback. Incorporation of Medical Director comments.
16.12.19	V3	Andrew Fletcher (IGMAG Policy Sub Group)	Review of control standard text, review of structure, refinement of sections, updates to references in line with GDPR
22.02.22	V3.1	Marcus Sandberg / Andrew Fletcher	Review
13.04.22	V4	Marcus Sandberg	Final
12.03.25	V4.1	Siân Howson	Review
02.06.25	V4.2	Siân Howson	Review and inclusion of data protection principles, update to references, removal of sign-up sheet, replacing with an online form.
04.08.25	V5.0	Siân Howson	Final

Authorisation

Signing of this document indicates acceptance of its contents

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

Appendices: Supporting the Control Standard for electronic health and care records (supplementary information and guidance)

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)

Appendix 1 Supplementary Information and Guidance

A. Wales Accord on the Sharing of Personal Information (WASPI) (Section 2 - Purpose)

WASPI is the national accepted information sharing framework in Wales. It provides a set of principles and template documents that help organisations to comply with their obligations under Data Protection legislation and the Information Commissioner's Data Sharing Code of Practice.

Whereas information sharing agreements within the WASPI framework are focused on the purposes of sharing the information and the detail of personal data shared; the 'who, why, where, when, what and how', the Control Standard sets out specific requirements around the systems used to share the information. The Control Standard does not negate the need for a WASPI information sharing agreement, where relevant.

Further information on WASPI can be found on the frameworks website - WASPI Home - Welsh Accord on Sharing of Personal Information

B. Legal considerations (Section 4 – Example Mechanisms for the Sharing of Personal Data)

When considering whether a proposal to share data is lawful, it is first necessary to consider whether the parties to the proposed arrangement have the necessary powers.

A public body may only share data if it has power to do so. The power may be set out expressly in statute, or it may be implied from the body's other statutory powers and functions. It is also important to ascertain whether there are express statutory restrictions on the data sharing activity proposed, or any restrictions which may be implied by the existence of other statutory, common law or other provisions.

For organisations providing NHS Wales services in Wales, the following sections of the National Health Service (Wales) Act 2006 may be relevant:

- Section 1 places a duty on the Welsh Ministers to continue the promotion of a comprehensive health service designed to secure improvement in the physical and mental health of the people of Wales, and in the prevention, diagnosis and treatment of illness. Section 2 of the Act empowers Welsh Ministers to do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

- Section 3 provides that Welsh Ministers have a statutory duty to, inter alia, provide throughout Wales, to such extent as they consider necessary to meet all reasonable requirements,

healthcare services and such other services or facilities as they require for the diagnosis and treatment of illness.

- Section 12 states the Welsh Ministers may direct a Local Health Board to exercise in relation to its area functions relating to the health service. Pursuant to the Local Health Board (Directed Functions) (Wales) Regulations 2009, the duty under Section 3 of the 2006 Act has been delegated to the Local Health Boards and are thus responsible for the provision of health services in Wales.

- Section 18 provides that Welsh Ministers may by order establish NHS trusts to provide goods and services for the purposes of the health service. Section 19 of the National Health Service (Wales) Act 2006, the Welsh Ministers may give directions to an NHS trust about its exercise of any functions.

- Section 22 states that Welsh Ministers may by order establish special bodies, known as a Special Health Authorities, for the purpose of exercising any functions which may be conferred on them.

- Section 24 provides the Welsh Ministers may direct a Special Health Authority to exercise any of the functions of the Welsh Ministers relating to the health service which are specified in the directions. Section 23 of the National Health Service (Wales) Act 2006 provides that the Welsh Ministers may give directions to a Special Health Authority about its exercise of any functions.

The legislation outlines key data protection principles which must be adhered to. These include:

- **Lawfulness, fairness and transparency**: ensuring that data is processed lawfully, fairly and in a transparent manner relating to the data subject

- **Purpose limitation:** ensuring that data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall (in accordance with UK GDPR Article 89(1)), not be considered to be incompatible with the initial purposes

- **Data minimisation:** ensuring that data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

- **Accuracy:** Ensuring that the data processed is accurate and, where necessary, kept up to date; organisations will ensure that every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- **Storage limitation:** ensuring that the personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be

processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with UK GDPR Article 89(1) subject to implementation of the appropriate technical and organisational measures required by UK GDPR in order to safeguard the rights and freedoms of the data subject

- **Integrity and confidentiality:** Ensuring that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

- **Accountability**: each organisation will be responsible for, and be able to demonstrate compliance with, UK GDPR Article 5(1)(a-f).

C. Staff responsibilities (Section 6 – Access and Appropriate Use)

Staff of all organisations must:

a) Be responsible for their own actions including using, collecting, storing, accessing and disclosing or sharing information;
b) Only access and use the information to support their role within the direct care and wellbeing of the service user;
c) Be open and transparent with the service user about the use of their information;
d) Maintain the service users' record to professional and records management standards;
e) Undertake regular training in information governance, the use of information and the relevant information systems and applications.

D. Terms of Access to shared electronic health records (Section 6 Access and Appropriate Use)

Where electronic records are maintained, these are held on secure NHS computer systems access to NHS Wales's computer systems is permitted by trained and authorised personnel only. The security measures in place will be designed to guarantee that all service user information is treated as sensitive and confidential. Methods and procedures for secure access are under continual review in order to sustain a technical improvement process.

In addition to the processes described in this section IT solutions will be required to manage these processes; these may be implemented at a local or national level.

E. Role based access and controls (Section 6 – Access and Appropriate Use)

Role based access controls is a key requirement for systems that share electronic health records on the principle that a staff member must only have access to information in line with their role. Role based access provides a manageable, scalable approach to access control. Principles which should be considered adopting and developing any role base access models are:

- Keep it simple;
- Confidence is heavily based on trust;
- Access to information always on a 'need to know' basis.

In development of user roles it may be a necessity to group users together with a common set of access privileges i.e. each user access role will provide a set of users with the same levels of access to the same types of data. Generally, these will relate to the degree of access to patient information required and for example, whether read only or update access is required.

F. Management of user accounts (Section 6 – Access and Appropriate Use)

Maintenance of accurate user account information is the 'joint/shared' responsibility of the individual user and the organisation which granted user access. The method employed to manage accounts is a local decision, but it must have clearly defined roles and responsibilities.

In addition to any joint working agreements local procedures should exist to address the adding/deleting and maintaining of user registration details. These procedures should clearly describe the roles and responsibilities of all those party to the agreement in maintaining accurate user account information and in providing access to shared records.

Access must be controlled by a unique user name and password that meets the minimum NHS Wales Standard for strong authentication at the appropriate e-Gif level. Password management and other access security must comply with the specifications set out in the International Standard for Information Security Management Systems ISO27001 and follow relevant policy.

G. Data Quality (Section 7 – Individual Rights)

All those involved in the care of a service user need to be able to rely on the accuracy of the available information in order to be able to provide timely and effective treatment or care for that individual, maintain the integrity of service user information and to minimise risk. This becomes even more important as we move into the world of shared electronic records.

Examples of when checks can be made to ensure data quality include:

- Where a service user attends an appointment;
- If a service user rings a call centre for booking appointments;
- When referrals are received; or
- On admission (for secondary care services or treatment).

H. Duplicate records and the role of the Master Patient Index (Section 7 – Individual Rights)

A number of duplicate or confused records can occur where service users have the same forename, surname, date of birth, and postcode.

The Master Patient Index (MPI) is a Welsh system that makes it easier to ensure patients are correctly identified and minimises the number of duplicate health records held for each patient.

There are large numbers of duplicate records identified within the MPI. Many of these duplicates are historical and relate to patients who are now deceased or have moved away, however, new duplicate records continue to be created at a steady rate.

The criteria stated in the standard will minimise the risk of creating duplicate records.

Reports are available identifying potential data quality problems within Health Board/Trust records.

This includes:

- Recently registered records which are duplicates;
- Recently registered records which are potentially duplicates;
- Records for patients which have recently been flagged as deceased on WDS but are not flagged as deceased on the Health Board/Trust system;
- Records with a date of birth that differs from the WDS date of birth for the same patient.

I. National Intelligent Integrated Auditing Solution (Section 8 Auditing and Assurance)

Auditing of user access is essential to ensure that those with access to service user information are held accountable. To enable this the National Intelligent Integrated Auditing Solution (NIIAS) will be applied to the Shared Electronic Health Records, which will produce access logs enabling scrutiny of every access to the record.

These automated audits are a requirement under the NHS Wales Information Governance Toolkit, in order to provide the assurance that patient confidentiality is being maintained.

The software:

- Simplifies the analysis of access logs taken from clinical systems;
- Makes it easier to generate reports;

- Detects and alerts Information Governance to potentially unauthorised access to electronic systems that hold patient information;
- Highlight unusual or suspicious activity for further investigation;
- Enable investigation of accesses to specific patients' records;
- Makes sure staff, who may also be patients at some point in time, can be reassured in the knowledge that their patient record is also protected by this software.

NIIAS scrutinises each access of the Shared Electronic Health Record and have the ability to filter information according to the agreed policies set out below. The purpose of the generated outputs is to assist in determining breaches against policy where a user has accessed information they are not entitled to view. These accesses will be subject to the following reports:

- **Historic records** – staff member has access a patients historic health record without first accessing a more recent record;
- **Same surname** – staff member has access multiple health records with the same surname;
- **Own record** – staff member has access his or her own health record;
- **Family members** – events where a staff member has accessed patient records for a family member;
- **Person of interest** – staff member has access the health record of a person of local or national media interest;
- **Work colleagues** – staff member has accessed the health record of a work colleague.

NHS Wales Organisations must ensure they have the resource and skillset to actively use and manage NIIAS, and that users are supported through a bespoke support network.

J. Records Management Code of Practice for Health and Social Care 2022 (Section 9 – Records Management)

The Records Management Code of Practice for Health and Social Care 2022 ("the Code") is a guide for organisations to use in relation to the practice of managing records.

The Code is based on the Records Management Code of Practice for Health and Social Care 2021 developed by NHSX in England, and provides a framework for consistent and effective records management based on established standards and current legislation.

It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management system including advice on organising, storing, retaining and deleting records. It applies to all records regardless of the media they are held on.

By aligning local policies to this Code, organisations are demonstrating appropriate records management of corporate and health records.

K. Policies, procedures and reporting of incidents (Section 10 – Policy, Incidents and Complaint Management)

An Information Governance (IG) incident is any incident which involves actual or potential failure to meet the requirements of Data Protection legislation, the common law duty of confidence or any other legislation as may be relevant to that information. This includes unlawful disclosure or misuse of confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.

Organisations recognise that damage resulting from potential and actual serious incidents and/or information security events should be minimised and lessons learnt from them. To this end, all security incidents will be reported as soon as they are confirmed, recorded and investigated and appropriate actions taken to address the incident and learn lessons (where possible) so that they do not recur. This includes weaknesses identified in systems design or operational procedures that potentially may result in an information security incident.

Organisations will refer to "Putting Things Right", including providing "early warning" notifications to Welsh Government. Early warning notifications should be used in circumstances where the Welsh Government needs to be alerted to an immediate issue of concern or provided prior warning where there may be potential impact which may affect Welsh Government or NHS Wales. Organisations will also notify the Information Commissioner's Officer where required to under Article 33 of UK General Data Protection Regulation (UK GDPR) and / or any data subjects under Article 34 UK GDPR.

Dependent upon the nature of the incident, notification will also be sent to other relevant organisations where they are acting as joint controllers or independent controllers working together.

Appendix 2

In this Agreement the following words have the following meanings:

Term	Definition
Audit trail / log	An audit trail (or audit log) is a record access to and changes made to a record, why and when they did so and what changes were made.
Data breach	Unlawful disclosure or misuse of personal confidential data and an inappropriate invasion of people's privacy.
Data controller	A person (individual or organisation) who determines the purposes for which and the manner in which any personal confidential data are or will be processed. Data controllers must ensure that any processing of personal data for which they are responsible complies with the Data Protection legislation. Joint Data controllers agree to share a pool of personal data that they process independently of each other.
Data processor	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Designated Person	A senior manager within the organisation who will have responsibility for ensuring the commitments under the Control Standard are implemented, monitored, understood and acted upon by relevant practitioners and that access to personal information is regularly monitored and audited to ensure appropriate access is maintained.
Direct Care	A clinical or public health activity concerned with the diagnosis, prevention, investigation and treatment of illness.
UK General Data Protection Regulation	Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
Information Governance	How organisations manage the way information and data are handled within the NHS. It covers the collection, use, access and decommissioning as well as requirements and standards which organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.
Legitimate relationship	The relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care

Practitioners	An inclusive term to describe any staff working for the partner organisations involved in the care of or provision of services for the service user.
Service user	Any person receiving health or social care services, for example the patient.
Service user record	An electronic or paper record containing information about a person for the purpose of managing their healthcare.
Senior Information Risk Officer (SIRO)	An Executive or Senior Manager on the Board who is familiar with information risks and the organisation's response to risk. The role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Board.
Third parties	In relation to personal data, any person other than the subject of the data, the data controller, or a data processor.