Health Education and Improvement Wales (HEIW)

Data Protection and Confidentiality Policy

Policy Owner: Head of Cyber Security & Information Assurance
Approved by: Executive Team
Issue Date: 29 January 2025
Review Date: 29 January 2028
Date of EIA Outcome: 9 September 2024

Contents

1. Policy Statement 3
2. Scope 3
3. Aims and Objectives 3
4. Roles and Responsibilities 3
5. Policy 5
    5.1. Processing Personal Data 5
    5.2. Lawful Basis 6
    5.3. Individual Rights 7
    5.4. Purpose Limitation 8
    5.5. Data Minimisation 8
    5.6. Accuracy of Personal Data 8
    5.7. Records Management, Storage and Retention 8
    5.8. Information Security 9
    5.9. Accountability 9
    5.10. Confidentiality 9
    5.11. Data Protection Impact Assessment (DPIA) 9
    5.12. Reporting of Confidentiality Breaches 10
    5.13. Privacy Notices 10
    5.14. Information Assets 10
    5.15. Information Sharing 11
    5.16. Information Transfer and Security 11
    5.17. Subject Access Requests (SAR's) 11
    5.18. Training and Awareness 12
    5.19. Contracts of Employment 12
    5.20. Social Media 12
6. Definitions 12
    6.1. Personal Data 12
    6.2. Special Category Data 13
    6.3. Personal Data Breach 13
    6.4. Processing. 13
    6.5. Misdirection 13
7. Equality Impact Assessment 13
8. References 14
9. Getting Help 14
10. Legislation and Standards 14
11. Related Policies and Procedures 15
12. Publication and Dissemination of Organisation Wide Documents 15
13. Compliance 15
14. Policy Review 16

1. Policy Statement

HEIW processes a wide range of personal data relating to individuals and in doing so must fulfil its legal obligations set out in data protection legislation. Personal data refers to any information relating to an identified or identifiable living individuals.

The processing of personal data must comply with data protection legislation. HEIW therefore regards the correct and lawful processing of personal data as vital and will ensure that it processes personal data in accordance with data protection legislation.

For the purposes of this policy HEIW takes the view that the principles of confidentiality apply to all personal data it processes and, in any form, (e.g., held electronically on a computer, held physically on paper or communicated electronically, verbally or in writing). This policy sets out the high-level intent of HEIW.

2. Scope

This policy applies to HEIW's workforce (all staff) including permanent staff, fixed-term, students, trainees, secondees, volunteers, contracted third parties, agency and any persons undertaking duties on behalf of HEIW. This policy applies to all personal data being processed throughout HEIW and its directorates regardless of how the data is created or processed.

3. Aims and Objectives

The aim of this policy is to set out key areas of responsibility and HEIW's commitment to ensuring it fulfils its legal obligations set out in data protection legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA 2018)

4. Roles and Responsibilities

The **Chief Executive Officer** (CEO) is responsible for ensuring the highest level of organisational commitment to the policy and the availability of resources to support its implementation and any associated legal requirements. Responsibilities may be delegated to HEIW and Senior Information Risk Officers, Data Protection Officers, and/or Caldicott Guardians as appropriate.

The **Senior Information Risk Owner** (SIRO) is responsible for information risk management across the organisation. The SIRO is responsible for taking ownership of the organisation's information risk policy and advocating good information risk management and practice. The SIRO reports to the Chief Executive Officer (CEO) and is accountable to the Board. HEIW's nominated SIRO is the Board Secretary.

The **Caldicott Guardian** is responsible for protecting the confidentiality of health and care information held by their respective organisation and enabling appropriate information sharing by ensuring that information is used properly. Together with the respective Senior Information Risk Officer, they are responsible for monitoring the process by which all information assets are identified, created, managed and reviewed. Although HEIW does not deal with patient information it has been agreed this role shall be held by the Medical Director.

The **Data Protection Officer** (DPO) reports to the Chief Executive Officer (CEO) and is accountable to the Board. The DPO will provide oversight of HEIW compliance with data protection legislation and informing the organisation on its data protection obligations. As a data protection expert, the DPO must maintain expert knowledge of data protection laws and practices and how these apply to an organisation. The DPO will be the primary point of contact within the organisation regarding data protection matters, whilst advising senior management on the development and establishment of policies, standards, procedures, and other measures to ensure effective governance and compliance with data protection legislation. HEIW's nominated DPO is the Director of Digital, Data and Engagement.

Executive Directors are responsible for the management of information risk within their service areas and are responsible for ensuring their staff and managers comply with this policy.

Managers are responsible for the implementation of this policy within their departments. In addition, they must ensure that their staff comply with this policy, understand their responsibilities and are up to date with mandatory information governance, records management, and cyber security training. Breaches of the policy must be reported via local incident reporting processes and dealt with in line with the HEIW Disciplinary Policy where appropriate.

The **Information Governance** team has a delegated responsibility from the DPO to discharge its duties and carry out necessary operational work to ensure compliance with data protection legislation, NHS Wales policies, standards, procedures, and codes of practice. These responsibilities also include compliance and monitoring. The Information Governance team are responsible for providing appropriate information governance advice and support to Information Asset Owners (IAO's), Service Leads, staff, and managers to ensure the policy is understood and complied with.

The **Cyber Security** team are responsible for providing subject matter expertise and guidance on appropriate controls and measures to protect information and information systems.

Information Asset Owners (IAO's) are responsible for understanding what information is held within their service areas and for ensuring that this policy is being applied to their information assets by staff and managers. They are responsible for deciding upon the classification levels of information within their service or information asset area with support from subject matter experts such as the Information Governance or Cyber Security team where required. They can delegate this responsibility to another named individual, but they must retain overall responsibility for the information asset and the correct application of this policy to that asset.

All staff must familiarise themselves with the policy content and ensure the policy requirements are implemented and followed within their own work area. Policy content should be read with other related policies outlined in section 11. Mandatory information governance, records management and cyber security training must be undertaken at least every two years. Breaches of this policy must be reported via local incident reporting processes.

All staff are required to respect the personal data and privacy of others and must ensure that appropriate protective and security measures are taken to protect against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to all personal data.

All staff must adhere to all confidentiality requirements as described by HEIW and ensure that any access and use of personal data is only ever for the purposes of fulfilling NHS Wales duties.

5. Policy

5.1. Processing Personal Data

Under data protection legislation it is HEIW's legal obligation to process all personal data in compliance with the UK GDPR lawfulness, fairness, and transparency principle.

This means that HEIW will:

- Identify, confirm, and communicate its lawful basis under the UK GDPR to process individuals' personal data.
- Process individuals' personal data in a manner which is fair and in ways that individuals would reasonably expect their personal data to be processed and to not process personal data in ways that could have detrimental effects on individuals.

- Be transparent about its processing with individuals to ensure HEIW is clear, open, and honest with individuals about who we are and how and why HEIW is processing individuals' personal data.

5.2. Lawful Basis

The lawful basis for the processing of personal data are set out in Article 6 of the UK GDPR. At least one of the lawful basis for processing personal data must apply when processing personal data:

a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
d) **Vital interests:** the processing is necessary to protect someone's life.
e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

Where special category data us processed, there are 9 conditions for processing set out in Article 9 of the UK GDPR, these include:

a) Explicit consent.
b) Employment, social security, and social protection (if authorised by law).
c) Vital interests.
d) Not-for-profit bodies.
e) Made public by the data subject.
f) Legal claims or judicial acts.
g) Reasons of substantial public interest (with a basis in law).
h) Health or social care (with a basis in law).
i) Public health (with a basis in law).
j) Archiving, research, and statistics (with a basis in law).

If an organisation is relying on conditions **(b)**, **(h)**, **(i)** or **(j)**, they will also need to meet the associated condition in UK Law, set out in **Part 1 of Schedule 1** of the DPA 2018.

If an organisation is relying on the substantial public interest condition set out in Article **9(2)(g)**, they will need to meet one of **23** substantial public interest conditions detailed in **Part 2 of Schedule 1** of the DPA 2018.

5.3. Individual Rights

Individuals have the right to be informed about the collection and use of their personal data and the processing of their personal data. These rights include:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restricted processing
- Right to data portability
- Right to object
- Rights related to automated decision-making including profiling

HEIW shall ensure that appropriate arrangements are in place to manage these rights. All staff must follow local policies, procedures, and guidelines to ensure that requests relating to individuals' rights (e.g., such as the right of access) are managed appropriately.

In some cases, HEIW may refuse to comply with a request (or part of a request) invoking individual rights if an exemption applies, or if the request is considered manifestly unfounded or manifestly excessive.

The ICO has documented detailed guidance explaining how exemptions apply and factors to be considered in deciding as to whether a request is considered manifestly unfounded or manifestly excessive.

- A guide to individual rights | ICO
- When can we refuse to comply with a request? | ICO

If HEIW refuses to comply with a request or part of a request, the individual must be informed of the reasons why the request was refused, their right to make a complaint to the ICO or another supervisory authority and their ability to seek to enforce their right through the courts.

5.4. Purpose Limitation

HEIW shall be clear and transparent about its reasons for obtaining and processing individuals personal data. HEIW shall record its purposes for processing personal data and will inform individuals in documented privacy notices.

5.5. Data Minimisation

HEIW will ensure the personal data it processes is adequate, relevant, and only limited to what is necessary for its processing arrangements. HEIW will use the minimum amount of identifiable information when processing personal data. All staff must follow policies, procedures, and guidelines to ensure the principle of data minimisation is upheld.

5.6. Accuracy of Personal Data

HEIW shall put arrangements in place to ensure the personal data it processes is accurate and up to date. All staff must follow all relevant policies, procedures, and guidelines to ensure that personal data is appropriately maintained and accurate.

5.7. Records Management, Storage and Retention

HEIW's Records Management Policy sets out key areas of responsibility and affirms our commitment to achieving high standards in records management.

As a Special Health Authority (SHA), the correct management of records is a legal and compliance matter under Data Protection Legislation (UK GDPR and DPA 2018); the Freedom of Information Act 2000 (FOIA); and the Public Records Act (PRA).

Information is a valuable commodity and essential to HEIW's day-to-day operations, carrying out its role and statutory functions. HEIW receives, creates, manages, and processes a significant volume of information and in a range of formats (e.g., electronic, physical).

Appropriate and effective records management is therefore considered a critical business activity, to ensure that records and the information they contain are appropriately managed, accurate, up-to-date, and available to authorised individuals when required, and in a way which conforms with HEIW's legal obligations.

5.8. Information Security

HEIW shall put in place reasonable and proportionate controls (i.e., management, operational, technical) to maintain the confidentiality, integrity and availability of information and information systems.

5.9. Accountability

HEIW is accountable for the personal data it processes day-to-day and is responsible for complying with data protection legislation (e.g., UK GDPR) and demonstrating its compliance. To ensure this, HEIW shall put in place management, operational and technical controls to meet its accountability requirements.

5.10. Confidentiality

All staff have an obligation of confidentiality regardless of their role and are required to respect the personal data and privacy of others in line with data protection legislation, common law duty of confidence, Caldicott Principles, All Wales policies, local policies, procedures, and guidelines.

5.11. Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment (DPIA) is a process to help identify, assess, and manage data protection and privacy risks which are associated with a project or plan.

DPIA's are an essential part of HEIW's accountability obligations under the UK GDPR. Carrying out a DPIA is a legal requirement for any type of personal data processing, including processing that is likely to result in a high risk to individuals' rights and freedoms.

Considering data protection risks is an essential component of 'data protection by design' principles. Completing DPIA's increases the awareness of potential data protection and privacy risks and ensures that all staff involved in projects are considering privacy from the commencement of a project.

All new projects or major new flows involving personal data must consider information governance and privacy practices from the outset and therefore require a DPIA. Project Leads are responsible for ensuring a DPIA is completed and approved.

5.12. Reporting of Confidentiality Breaches

HEIW takes any potential breach of confidentiality very seriously. All staff must report any breach of this nature to their line manager and the Information Governance team and within 24 hours of breach identification. All staff are expected to follow the documented Breach Reporting Procedure.

5.13. Privacy Notices

HEIW holds and processes personal data and as such requires privacy notices. A privacy notice also known as a privacy policy lets individuals know what HEIW is doing with their personal data.

Providing a privacy notice is a key requirement of the UK GDPR to ensure transparency and to explain to individuals:

- The types of personal data we collect about individuals.
- How we collect personal data, why we need it and how we use it.
- The lawful basis we have for processing personal data.
- When and who do we share personal data with.
- How we secure personal data.
- How long we hold personal data for.
- Use of cookies, other technologies and the use of automated decision making and profiling.
- Individuals' legal rights in relation to personal data.
- How to contact us, including how to make a complaint with the supervisory authority.
- When the privacy notice was last updated.

Privacy notices must also include HEIW's full contact details, individuals' rights under data protection legislation and details on how to make a complaint.

5.14. Information Assets

It is the policy of HEIW to ensure that all personal data and commercially sensitive information it processes is identified, catalogued, classified, recorded, and appropriately managed. To accomplish this, information assets will be systematically catalogued and managed using an Information Asset Register (IAR).

All information assets recorded on IAR's shall be assigned to an appropriate Information Asset Owner (IAO) to ensure that information assets are appropriately managed throughout the information asset lifecycle.

5.15. Information Sharing

Such sharing may take place between the public services and appropriate private and third sector service providers. Sharing must take place legally, safely and with confidence to ensure public services are maintained and in order to improve standards and efficiency.

The Wales Accord for the Sharing of Personal Information (WASPI) is a framework under which information sharing protocols are formed where a regular sharing of personal data is to take place. HEIW has 'signed up' to use this framework and therefore in all instances of regular information sharing an Information Sharing Protocol should be adopted using the WASPI model.

5.16. Information Transfer and Security

All staff must pay particular attention to any need to transfer and communicate personal data via any form of telecommunication and/or data transportation methods. HEIW expects this type of information to be communicated with due care and adequate protection.

In accordance with local policies and procedures, all staff must ensure that suitable precautions are applied when personal data is transferred.

All staff must ensure that appropriate protection and security measures are put in place to protect against unlawful or unauthorised access or disclosure of personal data when there is a need to convey any personal data to internal or external parties.

All staff must ensure that the correct recipient details are selected to avoid the potential consequences of misdirection and/or accidental disclosure of personal data.

All staff are required to read and comply with the All Staff - Information Handling Rules.

5.17. Subject Access Requests (SAR's)

Data protection legislation establishes a framework of rights and duties designed to safeguard personal data. Individuals (known as data subjects) or their representatives have a right to apply for access to information held about them. This is known as a Subject Access Request (SAR).

The DPO and Information Governance team will ensure that all SAR's are handled appropriately, and in accordance with data protection legislation.

5.18. Training and Awareness

HEIW will ensure that adequate training is provided to all staff involved in the processing of personal data and that qualified expertise is available for consultation.

All new starters shall undertake mandatory ESR information governance, records management, and cyber security training as part of the HEIW induction process.

All staff shall undertake mandatory ESR information governance, records management, and cyber security training every two years.

All staff who require support in understanding the legal, professional, and ethical obligations that apply to them should contact the Information Governance team.

5.19. Contracts of Employment

All contracts of employment must include a data protection and general confidentiality clause. Agency, contractors, and non-contract staff working on behalf of HEIW are subject to the same rules.

5.20. Social Media

Social media is a term for websites based on user participation and user-generated content. These media provide a number of benefits for HEIW as they are recognised as a valuable tool and provide another platform in which to engage with service users, to promote HEIW.

It is the responsibility of all staff employed or engaged by HEIW to comply with the All-Wales Social Media Policy.

6. Definitions

6.1. Personal Data

Personal Data is defined in the UK GDPR as:

"'Personal Data' means 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".

6.2. Special Category Data

Some personal data can be more sensitive in nature and thus requires a higher degree of protection. The UK GDPR defines this type of data as 'special category data' which include:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership.
- genetic data.
- biometric data (where used for identification purposes).
- data concerning health.
- data concerning a person's sex life.
- data concerning a person's sexual orientation.

6.3. Personal Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

6.4. Processing

Processing in relation to personal data means the operations which are performed on personal data (this includes automated means) such as the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, disclosure, dissemination, restriction, erasure, or destruction.

6.5. Misdirection

Misdirection is the term associated with the accidental sending of personal data via methods to include emails, letters, and faxes. Whether or not the sending of personal data is sent internally or externally, misdirection is a main risk to HEIW. Accidental misdirection may result in a breach of confidentiality if the content identifies a living individual (e.g., members of staff, trainees).

7. Equality Impact Assessment

After seeking pertinent advice from HEIW's Equality, Diversity and Inclusion team, it was agreed the content of this policy is mandatory and outlines HEIW's legal and organisational responsibilities in respect of appropriate records management. Procedures underpinning and supporting the implementation of this policy shall be assessed against accessibility and usability to ensure they do not have a negative impact on individuals with protected characteristics.

8. References

Links to the Information Commissioners Office (ICO) also provide a valuable source of information:

Information Commissioner's Office (ICO)

9. Getting Help

For further advice or assistance on how to ensure compliance with this policy, please contact the Information Governance team.

Information Governance team: HEIW.InformationGovernance@wales.nhs.uk

10. Legislation and Standards

- UK General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000

Relevant Codes of Practice and Standards include, but are not limited to, the following:

- Caldicott Principles
- Information Security ISO/IEC 27001
- Information Commissioners Codes of Practice
- NHS England Records Management Code of Practice 2021 (formally NHSX)
- Welsh Government Records Management Code of Practice for Health and Social Care 2022

Other references include:

- Privacy and Electronic Communications Regulations 2003
- Public Records Act 1958 / 1967
- Computer Misuse Act 1990
- Copyrights, Designs & Patents Act
- Human Rights Act 1998
- Fraud Act 2006
- The Regulation of Investigatory Powers Act 2000
- Common Law - Duty of Confidence
- Information Governance Assurance Programme Guidance 2008-9
- Data Protection (Processing of Sensitive Personal data) Order 2000

- The Caldicott Report 2013
- Professional Codes of Conduct

11. Related Policies and Procedures

This policy should be read in conjunction with the following HEIW policies:

- All Wales Information Governance Policy
- All Wales Information Security Policy
- All Wales Email Use Policy
- All Wales Internet Use Policy
- All Wales Social Media Policy
- Records Management Policy
- Information Asset Procedure
- Breach Reporting Procedure
- Subject Access Request Procedure
- Freedom of Information Act Policy

12. Publication and Dissemination of Organisation Wide Documents

The Board Secretary is responsible for publishing email notices regarding newly approved organisation-wide documents.

The Senior Management team is responsible for notifying staff of the document's publication and ensuring they have access to such documents so that they can be implemented as necessary by staff in their daily role.

13. Compliance

Guidance on the policies and procedures necessary to comply with this policy will be made available to all staff. Managers will be responsible for ensuring that all their staff are made aware of HEIW policies, procedures, and work instructions.

HEIW trusts its workforce, however it reserves the right to monitor work processes to ensure the effectiveness of the service. This will mean that any personal activities that the employee practices in work may come under scrutiny. HEIW respects the privacy of its workforce and does not want to interfere in their personal lives but monitoring of work processes is a legitimate business interest.

Staff should be reassured that HEIW takes a considered approach to monitoring; however, it reserves the right to adopt different monitoring patterns as required. Monitoring is normally conducted where it is suspected of a policy or legislation breach. Furthermore, on deciding whether such analysis is appropriate in any given circumstances, full consideration is given to the rights of the member of staff.

Managers are expected to speak to staff of their concerns should any minor issues arise. If breaches of information governance policies are detected an investigation may take place. Where information governance policies are found to have been breached, disciplinary procedures may be followed. Concerns about possible fraud and/or corruption should be reported to the Counter Fraud team.

In order for HEIW to achieve effective and good information governance, all staff must be encouraged to recognise the importance of information governance and report any data breaches or issues (including suspected breaches) to enable lessons learned.

Staff must be provided with the necessary tools, support, knowledge, and training to help them deliver their services in compliance with legislation. Ultimately a skilled workforce will have the confidence to challenge bad practices. This should minimise the risk of incidents and breaches occurring or recurring.

14. Policy Review

This policy will be reviewed every three years or more frequently where the contents are affected by major internal or external changes such as:

- Changes in legislation and/or regulation;
- Practice change or change in system/technology; or
- Changing methodology.