# Caldicott and Confidentiality Policy (Wales)

## Table of contents

# 1 Introduction

## 1.1 Policy statement

All staff working in the NHS are bound by a legal duty of confidence to protect personal information they may encounter during their work. This is not purely a requirement of their contractual responsibilities; it is also a requirement within the common law duty of confidence.

This policy also explains and enforces the obligations of confidentiality and non-disclosure among the employees of **Dulais Valley Primary Care Centre**. This applies to information generated, held and processed by the practice.

This policy is to be read in conjunction with the practice's privacy notices and an individual's contract of employment where this contains a confidentiality agreement.

Further information on privacy notices can be seen at Section 4.2.

Lastly, all staff are to fully understand the requirement to adhere to the Caldicott principles which are designed to safeguard and govern the use of patient information in all health and social care organisations.

## 1.2 Status

The practice aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the practice and other individuals performing functions in relation to the practice such as agency workers, locums and contractors.

## 1.3 Why and how it applies to them

This policy outlines the principles that are to be adhered to by all staff at **Dulais Valley Primary Care Centre** to understand the requirement for effective controls of personal confidential data (formerly patient identifiable information).

Staff are to be reminded that information classed as objective knowledge relates to the affairs of the practice. This may include information regarding partners, employees, patients, contractors, business associates, suppliers, market information, contractual arrangements, dealings, transactions, policies, procedures, decisions, technology and systems.

All employees must, from the beginning of their employment with the practice and after the termination of their employment with the practice, observe strict confidentiality and non-disclosure in respect of any information held by the practice except when required or authorised to disclose such information by the practice or by law.

The reputation and continuing ability of the practice to work effectively in the position of trust and responsibility it holds (which is also reflected in the trust and responsibility held by those persons engaged by the practice to work on its behalf) rely on confidential information being held as confidential. It must not be improperly disclosed and must be used only for the purpose for which such information was gathered.

Any breach of confidentiality, particularly involving data, could have major negative consequences for **Dulais Valley Primary Care Centre** and the individual. The practice will therefore take the appropriate disciplinary action against any employee who commits a breach of confidentiality by reporting it to the practice's Data Protection Officer (DPO).

If it is a serious breach, the DPO will be bound to recommend that it is reported to the Information Commissioner's Office (ICO) who may, in turn, institute criminal proceedings against the individual and, if found to be negligent, the practice itself. The individual, if found guilty, will be required to pay a fine and acquire a criminal record and the practice may be heavily fined if found guilty.

Nothing in this policy prevents an employee or other individual making a protected disclosure under the Public Interest Disclosure Act 1998 in respect of any malpractice or unlawful conduct.

The Caldicott principles are derived from the Dame Fiona Caldicott Information Governance Review in 2013 which now forms the current Caldicott Guardian guidance that was published in September 2021 from the National Data Guardian (NDG).

## 1.4 Legislation and guidance

In addition to the NDG guidance relating to the current Caldicott Guardian guidance, throughout this policy and any supporting references, the following legislation and guidance documents are referred to:

- The Caldicott Committee Report on the Review of Patient-Identifiable Information (1997)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Public Interest Disclosure Act 1998
- Caldicott review: Information: to share or not to share? The Information Governance Review
- The Health and Social Care Wales Act 2020
- Data Protection Act 2018 incorporating UK GDPR
- Caldicott Principles: A consultation about revising, expanding, and upholding the principles (2020)
- The Caldicott Principles (December 2020)

- Records Management Code of Practice (2021)
- Gender Recognition Act 2004
- Welsh Government Health and Care Standards
- Wales Safeguarding Procedures
- Social Services and Well-being (Wales) Act

### 1.5 Healthcare Inspectorate Wales

NHS Wales expects any practice to have a policy to support Caldicott and confidentiality processes and this should be used as evidence of compliance against Welsh Government Health and Care Standards. The Standards are the framework for inspections by the Healthcare Inspectorate of Wales.

Specifically, at Standard 3.4 **Dulais Valley Primary Care Centre** will need to ensure it can demonstrate the following measures are considered:

- Safe and secure information systems are developed in accordance with legislation and within a robust governance framework
- Processes exist to operate and manage information and data effectively, to maintain business continuity and support and facilitate patient care and delivery
- Data and information are accurate, valid, reliable, timely, relevant, comprehensible and complete
- Information is used to review, assess and improve services
- Information is shared with relevant partners using protocols when necessary to provide good care for people

Further information to support this standard can be found in the NHS Wales Governance eManual - Supporting Guidance.

## 2 Definition of terms

### 2.1 Data Protection Act and UK GDPR

The UK GDPR came into effect as of 1 January 2021, replacing the EU GDPR which had been in place since 25 May 2018. The UK GDPR is incorporated as Part 2 within the Data Protection Act 2018 (DPA18). Further reading can be found in the UK GDPR policy.

### 2.2 Confidentiality

The principle of keeping secure and secret from others, information given by or about an individual during a professional relationship.

### 2.3 Confidential information

Confidential information means any information processed by the practice or supplied (whether in writing, orally or otherwise) by the practice or gathered by an individual in relation to the performance of his/her duties that is marked as ‘confidential’.

Further details on confidentiality can be found in the NHS Wales Information security policy and NHS Wales Information governance policy for primary care service providers.

### 2.4 Protected disclosure

The protected disclosure of unlawful conduct, malpractice or wrongdoings within the practice is commonly known as 'whistleblowing (raising concerns)'.

### 2.5 Personal confidential data

As detailed within the NHS Wales Information security policy, this is information that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, etc.

### 2.6 Special category data

The UK GDPR singles out some types of personal data as likely to be more sensitive and gives these extra protection. These additions are called special category data and the special categories can be found in the ICO document titled What is special category data?

### 2.7 Caldicott principles

Caldicott principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

Further information on the Caldicott principles can be found at Section 3.11.

### 2.8 Caldicott Guardian

The Caldicott Guardian is to provide leadership and informed guidance on complex matters involving confidentiality and information sharing. This role is key to ensuring that **Dulais Valley Primary Care Centre** satisfies the highest practical standards for handling personal confidential data information.

### 2.9 UK Caldicott Guardian Council

The UK Caldicott Guardian Council (UKCGC) is the national body within the UK that provides support for Caldicott Guardians and others fulfilling the Caldicott function within the practice. This includes specific support for Caldicott Guardians during the COVID-19 pandemic.

The UKCGC helps to uphold the eight Caldicott principles.

### 2.10 British Medical Association

The British Medical Association (BMA) is the trade union and professional body for doctors in the United Kingdom.

### 2.11 Gender Recognition Act 2004

The Gender Recognition Act (GRA) 2004 contains specific guidance on how information about a patient's trans status can be shared. Further information on this subject can be found at Section 3.3.

### 2.12 Gender Recognition Certificate

After a minimum of two years and if certain key criteria are met, some trans people can apply for a Gender Recognition Certificate (GRC) under the GRA. If granted, the person acquires all the legal rights and responsibilities of their new gender and can obtain a new birth certificate. Further information on the GRC can be found at Section 3.4.

## 3 Guidance

### 3.1 Confidentiality

All employees must, from the date of the commencement of employment or other form of engagement, and thereafter, observe strict confidentiality in respect of any information held by the practice and by each individual working on behalf of the practice. This includes dealings, transactions, procedures, policies, decisions, systems and other matters of a confidential nature concerning the practice and its affairs.

Other than in the proper course of their duties, employees must not, either during or at any time after the termination of their employment, exploit or disclose confidential information. In addition, employees must not, through negligence, wilful misconduct, or inadvertence allow the use, exploitation or disclosure of any confidential information relating to the affairs of the practice, its patients, partners, employees, contractors, business partners or suppliers.

There must be no attempt to use any confidential information in a manner that may either directly or indirectly cause, or be calculated to cause, injury or loss to the practice.

### 3.2 Non-disclosure of information

It is an obligation upon all employees during employment, or engaged under other contractual arrangements, to maintain information in confidence and not, directly, or indirectly, disclose it other than for the purposes it was gathered. Any such information in the possession of an individual, either in electronic format or hard copy, shall be returned to the practice before or at the point in time that employment ceases, however such cessation occurs.

Following the cessation of employment, or other contractual engagement with the practice, an individual must not, directly or indirectly, use for gain, discuss or pass on to others confidential information that can be classed as objective knowledge in that it has been gained during their employment.

This includes information relating to:

- Partners

- Employees
- Contractors
- Patients
- Business associates
- Suppliers
- Market information
- Contractual arrangements
- Dealings
- Transactions
- Policies and procedures
- Decisions
- Technology and systems
- Any other matters relating to a confidential nature concerning the organisation

### 3.3 Protected information under the Gender Recognition Act

Section 22 of the GRA states that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.

This is classified as *protected information* and is defined in Section 22(2) as information relating to a person who has applied for a GRC under the Act, and which concerns that application (or a subsequent application by them) or their gender prior to being granted a full GRC.

Section 22 therefore is a privacy measure that prevents officials from disclosing that a person has a trans history.

However, there are exemptions from Section 22 for medical professionals. Statutory Instrument 2005 No.635 (Section 5) advises that it is not an offence to disclose information, provided all the following circumstances apply:

- The disclosure is made to a health professional
- The disclosure is made for medical purposes; and
- The person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent.

### 3.4 Trans status

Patients should never be asked to produce a GRC to 'prove' their trans status. The GRC is not a requirement and many trans people simply choose not to have one while others may not yet meet the eligibility criteria.

As a precautionary measure, it is good practice to apply the Section 5 criteria set out in Section 3.3 to all disclosures of information about the trans status of a patient. The reason being is that it may not be accurately known whether the person has a GRC or not. Additionally, the general protocols on medical confidentiality and information governance apply to all patients whether they have a GRC or not.

Pride in Practice has advised that it should be noted that good information governance around this subject is essential because unlawful and unwarranted disclosures of a person's

trans status leave organisations open to legal proceedings and can have serious and unforeseen consequences in 'outing' trans people.

Further reading on GRC and how one can be applied for can be found on Gov.uk here.

### 3.5 Third-party requests for information

Any employee approached by a third party, including any media source, and asked to make comments or provide information relating to the practice and its affairs (or the affairs of its patients, partners, employees, contractors, or any business associate) must not, under any circumstances, respond without having sought permission and guidance from **Lyn Jenkins, Practice Manager.**

The manager will then discuss the request with the partners and consider asking for assistance from the press information/media officer at the practice's Local Health Board.

### 3.6 Whistleblowing or protected disclosures

Legislation in the UK was enacted by the Public Interest Disclosure Act 1998 to enable employees and other persons such as temporary agency workers to disclose genuine concerns, especially those that seem to involve unlawful conduct or malpractice. The legislation also protects them from any form of victimisation arising from making such a disclosure.

In respect of any malpractice or unlawful conduct, any employee is entitled to submit a protected disclosure under the practice's Whistleblowing Policy which provides a procedure for making protected disclosures. This states that protected disclosures are normally made to **Lyn Jenkins.** If the individual employee feels unable to report the matter internally then they are free to report it to an external organisation.

This practice's external whistleblowing contact at Swansea Bay University Health Board is to whom concerns may be expressed.

Refer to the Whistleblowing (Raising Concerns) Policy

### 3.7 Confidentiality and non-disclosure agreement

All persons engaged to work for and on behalf of the practice will be required to sign the confidentiality and non-disclosure agreement to be found at Annex A. A signed copy will be held on the individual's personnel file.

Visitors to the practice will also be expected to sign a confidentiality agreement and this document also incorporates fire safety and risk awareness for visitors. Further information can be found at:

Third-party confidentiality agreement incorporating fire safety and risk awareness for visitors

## 3.8 Caldicott Guardian role

A Caldicott Guardian's role, as outlined within the Manual for Caldicott Guardians, is a senior person within a health or social care organisation who ensures that personal information about those who use its services is used legally, ethically and appropriately and that confidentiality is maintained.

The Caldicott Guardian's main concern is information relating to individuals and their care. Additionally, this need for confidentiality also extends to other individuals and this includes relatives, staff and others.

At **Dulais Valley Primary Care Centre** we store, manage and share personal information relating to staff and the same standards are applied to their information as are applied to the confidentiality of patient information.

Further information with regard to the role of the Caldicott Guardian and who practices need to appoint and their expected competencies can be sought in the NDG document titled Guidance about the appointment of Caldicott Guardians, their role and responsibilities.

## 3.9 Caldicott Guardian and/or Information Governance Lead

Practices are required to have their own Caldicott Guardian, and this is usually a senior clinician. This role is usually also given an additional title of Information Governance (or IG) Lead. Should a non-clinical person be appointed as the Caldicott Guardian, they should be supported by an appropriate clinician.

Further guidance on Caldicott Guardianship can be found at this Gov.uk site, although the Manual for Caldicott Guardians should be the starting point for those who are newly-appointed or as a reference point for existing Caldicott Guardians.

The Caldicott Guardian for **Dulais Valley Primary Care Centre** is Dr R L Jones.

## 3.10 Caldicott Guardian registration

The UKCGC states that all organisations that are required to have a Caldicott Guardian should ensure their up-to-date details are on the Caldicott Guardian Register.

## 3.11 Caldicott principles

In September 2020, it was agreed that the wording of the existing principles should be altered, and a further principle would be added.

This is detailed within the NDG document titled The Eight Caldicott Principles dated December 2020.

**Principle 1:**

Justify the purpose(s) for using confidential information. Every proposed use or transfer of confidential information should be clearly defined, scrutinised, and documented with continuing use regularly reviewed by an appropriate guardian.

**Principle 2:**

Use confidential information only when it is necessary. Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

**Principle 3:**

Use the minimum necessary confidential information. Where the use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

**Principle 4:**

Access to confidential information should be on a strict need-to-know basis. Only those who need access to confidential information should have access to it and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

**Principle 5:**

Everyone with access to confidential information should be aware of their responsibilities. Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

**Principle 6:**

Comply with the law. Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with the legal requirements set out in statute and under common law.

**Principle 7:**

The duty to share information for individual care is as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles.

They should be supported by the policies of their employers, regulators, and professional bodies.

**Principle 8:**

Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users so they can have clear expectations about how and why their confidential information is used and what choices they have about this. These steps will vary depending on the use.

As a minimum, this should include providing accessible, relevant, and appropriate information – in some cases, greater engagement will be required.

# 4 Compliance

All staff are to comply with the eight Caldicott principles and, should any doubt arise regarding compliance, they are to contact the Caldicott Guardian. The patients of **Dulais Valley Primary Care Centre** staff to uphold confidentiality at all times, doing so with confidence. **Dulais Valley Primary Care Centre** adheres to the NHS Wales Information governance policy and WASPI Framework. It is essential that patients are informed of the circumstances in which their personal confidential data may be shared in order to deliver safe and effective care.

Patients at **Dulais Valley Primary Care Centre** have a right to be informed of the intended use of their information and be given the choice to provide or withhold their consent (as appropriate). They also have an expectation that their information will be held securely and shared only with those directly associated with their care.

The four main requirements to maintain and improve a confidential service are:

1. **Protect patient information (A1)**

   Protect the patient's information through a number of measures:

   - Recognise that confidentiality is an obligation for all staff, external contractors and volunteers
   - Record patient information accurately and consistently
   - Keep patient information private
   - Keep patient information physically and electronically secure

2. **Inform patients effectively – no surprises (A2)**

   Ensure that patients are aware of how their information is used:

   - Check that patients have seen the available information leaflets
   - Make clear to patients when information is recorded, or health records are accessed
   - Make clear to patients when information is or may be disclosed to others
   - Check that patients are aware of the choices available in respect of how their information may be used or shared

- Check that patients have no concerns or queries about how their information is used

- Answer any queries personally or direct patients to others who can answer their questions or to other sources of information

- Respect the right of patients to have access to their health records

- Communicate effectively with patients to help them to understand

3. **Provide choice to patients (A3)**

    - Ask patients before using their personal information in ways that do not directly contribute to or support the delivery of their care

    - Respect patients' decisions to restrict the disclosure and/or use of information

    - Explain the implications of disclosing and not disclosing

4. **Improve wherever possible (A4)**

    - Be aware of the issues surrounding confidentiality and seek training or support when uncertain in order to deal with these appropriately

    - Report possible breaches or risk of breach

Furthermore, **Dulais Valley Primary Care Centre** will ensure that the foregoing requirements are strictly followed, and staff must ensure they report any breaches or risks to the the IG Lead immediately.

## 4.1 Welsh Information Governance Toolkit

The Welsh Information Governance Toolkit is an online self-assessment tool that enables **Dulais Valley Primary Care Centre** to measure its level of compliance against National Information Governance Standards and data protection legislation to ascertain whether information is handled and protected appropriately. This self-assessment will ensure compliance is in line with the General Data Protection Regulation (GDPR).

**Dulais Valley Primary Care Centre** will undertake an assessment to demonstrate that the practice can be trusted to maintain the confidentiality and security of personal information. To demonstrate compliance, **Dulais Valley Primary Care Centre** will submit an assessment no later than 30 September each year.

**Dulais Valley Primary Care Centre** will use the NHS Wales Information Governance Toolkit User Guide to ensure the practice achieves a successful outcome for the assessment. Reference should also be made to the Information Governance Website where further resources can assist with completion.

### 4.2 Practice privacy notices

The practice privacy notice explains to patients the ways in which the practice gathers, uses, discloses and manages a patient's data. It fulfils a legal requirement to protect a patient's privacy.

Other privacy notices are provided for the following:

- Children
- Employee
- Candidates applying for work

### 4.3 Audit

With the advances of technology in healthcare, it is imperative that access is monitored and controlled in an effectual manner. Regular audits must therefore be undertaken. This will ensure that access to confidential information is gained only by those who are required to access it in the course of their normal duties.

All staff at **Dulais Valley Primary Care Centre** have a responsibility to participate in such audits and to comply with the subsequent recommendations. Audit guidance and relevant templates can be found at Annex B and Annex C.

### 4.4 Additional compliance tools

In addition to audit, there are further tools that can be used to support such as:

- All members of the practice will undergo annual confidentiality training
- A confidentiality quiz is available at Annex D that can be used to promote staff understanding and their employee responsibilities when maintaining confidentiality
- A poster is available here which can be used within the practice or on the practice website to advise patients that **Dulais Valley Primary Care Centre** will ensure that their confidence will not be compromised if needing to discuss personal information that may be overheard.

## 5 Confidentiality in practice

### 5.1 Good practice

The following actions at **Dulais Valley Primary Care Centre** will be undertaken to ensure that confidentiality is maintained:

- Person-identifiable information will be anonymised so far as is reasonably practicable, whilst being mindful of not compromising the data
- Access to consulting rooms, administrative areas and record storage areas will be restricted

- All staff should always maintain a clear desk routine. No patient confidential information is to be left unattended in any unsecured area, at any time

- All IT equipment is to be shut down at the end of the working day except any that is required to remain left on such as server equipment

- Confidential waste is shredded or disposed of appropriately and as per the Confidential Waste Policy

- Staff will not talk about patients or discuss confidential information in areas where they may be overheard

The Communications Policy provides advice on disclosing information electronically or via telephone to a patient, proxy or third party.

### 5.2 Confidentiality breach

Any breach of confidentiality must be reported to the IG Lead. All breaches will be recorded and managed in accordance with ICO requirements.

This is further discussed in detail within the UK GDPR Policy.

### 5.3 Abuse of privilege

The NHS Confidentiality Policy states the following:

- It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends, or other persons without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018.

- When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility and contractual obligations and must undertake to abide by the policies and procedures of NHS England.

## 6 Disclosure

### 6.1 Disclosing information

The following list describes circumstances when information can be disclosed:

- When effectively anonymised in accordance with the ICO's Anonymisation Code of Practice

- When the information is required by law or under a court order. In this situation, staff must discuss the matter with their line manager or Information Governance staff

before disclosing who will then inform and obtain the approval of the Caldicott Guardian

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of Patient Information) Regulations 2002

- In child protection proceedings, if it is considered that the information required is in the public's or the child's interest. In this situation, staff must discuss the matter with their line manager or Information Governance staff before disclosing who will then inform and obtain the approval of the Caldicott Guardian

- When disclosure can be justified for another purpose; this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation, staff must discuss the matter with their line manager or Information Governance staff before disclosing who will then inform and obtain the approval of the Caldicott Guardian

- The patient both has the capacity to consent and consents to the disclosure. Further reading can be sought within the Consent Guidance

- It is a legal requirement to disclose certain communicable diseases. The full list of these notifiable diseases can be sought at Annex L to the Infection Prevention and Control Policy

# 7 Summary

Confidentiality compliance will be continually monitored, and any findings and subsequent recommendations will be discussed with staff.

It is important that all staff at **Dulais Valley Primary Care Centre** are conversant and comply with all matters concerning confidentiality. Failure to do so could have far reaching effects on the confidence that patients have in the practice staff and their relationship with health professionals.

Additionally, all staff must understand the importance of being aware of the action to be taken if they receive a request for information from third parties and the procedure to follow in the event that they wish to make a protected disclosure (whistleblowing).