Ref: IG13

CONFIDENTIALITY BREACH REPORTING POLICY

Executive Sponsor & Function:	Executive Director of Finance
Document Author:	Head of Information Governance
Approved by:	Quality, Safety and Performance Committee
Approval Date:	September 2025
Date of Equality Impact Assessment:	June 2025
Equality Impact Assessment Outcome:	Approved
Review Date:	September 2028
Version:	3

Contents Page

1. AIM

The aim of this policy is to ensure that the Trust reports all breaches which may take place in accordance with legislation, ICO Guidelines, NHS Wales Guidelines, Welsh Government Guidelines and best practice.

Achievement of these aims will detail how the Trust meets its legal obligations. It will further the commitment of the Trust to process all information in a manner that is aligned with applicable legislation. It will promote openness and demonstrate increased transparency of decision making thereby building public trust and confidence.

The policy also aims to provide all employees of the Trust with a framework in which to ensure that any breach is handled in accordance with current legislation, guidelines and best practice.

2. POLICY STATEMENT AND OBJECTIVES

Velindre University NHS Trust is responsible for protecting the information it holds and is legally required under data protection legislation to ensure the security and confidentiality of all patients, donors, staff and service users personal data being processed in the Trust.

This policy puts in place a standardised management approach throughout the Trust, it's respective divisions and associated organisations in the event of a personal data breach incident to ensure all such incidents are dealt with: -

- Effectively and efficiently;
- Recorded and reported in a consistent manner;
- Responsible officers and managers are alerted;
- To facilitate onward investigation; and
- To learn lessons to reduce the likelihood of a recurrence.

As such, this Policy sets out the high-level intent of the Trust and recognises the diversity of the respective Divisions and associated organisations under its control.

3. SCOPE OF THE POLICY

The Policy applies to all staff employed within the Trust regardless of status i.e. permanent, temporary, bank, agency, honorary contract holders and volunteers who process patient, donor, staff and service user personal data.

4. AIMS OF THE CONFIDENTIALITY BREACH REPORTING POLICY

The aim of this policy is to set out a clear process for the reporting of all personal data breaches and to ensure appropriate actions are taken in terms of communication and follow up to minimise the impact of any reported incidents.

4.1 Definitions

A personal data breach incident is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Data Breach incidents can be categorised[1] into three well-known security principles: -

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

Although not an exhaustive list, some common examples of a personal data breach incident, includes: -

- Accessing computer systems fraudulently, unlawfully without authorisation or using/sharing other employee NADEX logins, passwords, smart cards etc.
- Disclosing confidential information to individuals who have no legitimate right of access e.g. bogus callers, individuals not involved in service delivery and written requests from unauthorised requesters.
- Misdirection of email, faxes, letters and documents.
- The loss of paper files and computer print outs containing personal data.
- The loss of mobile/hardware devices due to crime or an individual's carelessness e.g. laptops, CDs, memory sticks, mobiles, iPads etc.
- The use of unauthorised systems and software such as Non-Corporate Communication Channels (NCCCs) (e.g. WhatsApp and similar) for business

4.2 Reporting Arrangements

Whenever a suspected personal data breach incident has occurred, it is imperative staff report the incident to their line manager without delay and at the latest within 24 hours of discovery and follow the Trust's Incident Reporting and Investigation Policy (including Serious Incidents) recording as much detail as possible of the incident into the Trust's Incident Reporting System, Datix.

More serious personal data breach incidents must be reported to key Trust staff e.g. Head of Information Governance (HOIG) and Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Caldicott Guardian, Chief Digital Officer, and the Information Governance (IG) Department. Early notification and preparation are key to dealing with management and investigation of reported personal data breach incidents to enable the Trust to meet its statutory obligations.

4.3 Personal Data Breach Investigation

The objective of any breach investigation is to identify what actions the Trust, its respective divisions and associated organisations need to take to first prevent a recurrence of the incident and second to determine whether the incident needs to be externally reported (i.e. to the Information Commissioner's Office).

[1] Guidelines on Personal data breach notification under UK GDPR 2018 - Article 33

Key to preventing any recurrence is to ensure the Trust, it's respective divisions and associated organisations learn from reported incidents, and where applicable, share lessons learnt and consider any trends and identify areas for improvement.

4.4 Incident Classifications

Personal data breaches should be classified according to severity of risk to such data in the table illustrated in **Appendix A**.

The Trust must have in place the appropriate means to regularly review personal data breach incidents which are and where necessary, cascaded within the appropriate Trust Board, Hosted Body, Divisional and associated organisational forums and Senior Leadership Teams.

4.5 Notifying individuals or other parties

Depending on the seriousness of the personal data breach, the Trust Board, Hosted Body, Divisions and/or associated organisations may be required to inform some or all of the following:

- The individuals concerned;
- The Information Commissioner's Office (ICO);
- Trust, Hosted Body, Divisional and Associated Organisational Senior Management, including the Chief Executive;
- Welsh Government (No surprises reporting);
- Associated organisations i.e. other NHS Wales Health Boards and Trusts;
- NHS Wales Counter-Fraud where fraud may be suspected
- Police.

Consideration must always be given to informing the individuals concerned or the next of kin of the affected individuals when information about them has been lost or inappropriately placed in the public domain.

4.5.1 Method of Notification

The method of notification will vary depending on the type and scale of the personal data breach and the availability of contact details of affected individuals.

In considering the most appropriate method of notifying a personal data breach, the Trust, Hosted Body, Divisions and/or associated organisations must ensure that no further confidential data is disclosed, i.e. sending notifications to the wrong home or email addresses.

4.5.2 The Information Commissioners Office (ICO)

The Trust, Hosted Body, Divisions and/or associated organisations will inform the ICO if the breach involves personal data and:

- Has been assessed in line with the ICO data breach reporting guidelines; or
- A statement is to be made to the Welsh Government and/or a media announcement is to be made; or
- The breach is likely to enter the public domain, to enable the ICO to prepare for any enquiries they might get.

There should be a presumption to report to the ICO where there is a large volume of personal data placed at risk, or the release of personal data could cause a significant risk of individuals suffering substantial harm. Every case must be considered on its own merits, however if unsure whether to report or not, then the presumption should be to report the breach.

The attached scoring system, at **Appendix B**[2], should be used to assist in determining the severity of an incident. Examples of applying the scoring system can be found at **Appendix C**.

Reporting to the ICO must be undertaken, without undue delay, and within **72 hours** of the Trust becoming aware of the personal data breach. Where notification is not made within 72 hours, it must be accompanied with reasons for the delay.

5. RESPONSIBILITIES

All staff have a role to play to ensure a safe and secure workplace and staff must be aware of this Policy to ensure care is taken at all times to protect information and avoid a personal data breach incident.

5.1 Managerial Accountability and Responsibility

The **Chief Executive** of the Trust has overall responsibility for ensuring compliance with applicable legislation and regulation.

The Trust has a legal obligation to appoint a **Data Protection Officer**, whose role is to undertake tasks to ensure appropriate measures are in place that safeguards personal data from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure in accordance with data protection legislation. The Trust's Head of Information Governance is the appointed Data Protection Officer.

Directors of Hosted Bodies and Divisions within the Trust are responsible for ensuring the Policy is implemented within their individual organisation, and must ensure: -

- Their organisation complies with this policy;
- Ensuring all staff and contractors are aware of the requirements incumbent upon them;
- Delegating the day-to-day responsibility to information governance leads and groups as defined by the Hosted Body/associated organisations and as appropriate to their needs.

The Trust has dedicated **Information Governance champions** in respective divisions and associated organisations. These roles will act as a first point of contact for receiving personal data breach incident notifications and act as an advisor to other managers and employees within their respective areas on compliance with the data protection legislation.

All staff are required to comply with this Policy and respect the personal data and privacy of others in their day to day working practice. Staff must ensure that

[2] Department for Health model as outlined in the Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation.

appropriate protection 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.

Non-compliance with this Policy and any employee who is found to compromise security or confidentiality of the Trust, its patients, donors, staff and/or service users may be subject to the Trust Disciplinary Policy.

6. LEGISLATION AND STANDARDS

This Policy is written in accordance with current legislation as well as relevant codes of practice and standards that include, but are not limited to, the following:

Human Rights

- European Convention on Human Rights
- Human Rights Act 1998

Rights to Privacy

- Investigatory Powers Act 2016
- Protection of Freedoms Act 2012
- Lawful Business Practice Regulations 2000

Data Protection

- Data Protection Act 2018 (includes UK GDPR)
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- Access to Health Records Act 1990
- Data (Use and Access) Act 2025

Online Privacy

- UK Privacy and Electronic Communications Regulations (PECR)
- UK Privacy and Electronic Communications Amendment 2012 (Cookie Law)

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

- Caldicott Principles
- Information Security ISO27001
- Information Commissioners Codes of Practice
- ICO's Employment Information Guidance
- Common Law Duty of Confidence

7. TRAINING AND AWARENESS

All new staff must attend an IG induction session upon appointment where appropriate training is given. This must be provided at the earliest opportunity and without delay.

Awareness sessions are scheduled regularly across the Trust and will inform staff of their responsibilities in relation to confidentiality of data, Freedom of Information Act

2000, Data Protection Act 2018 and Records Management in line with Section 46 Code of Practice on the Management of Records (FOI 2000). **All staff are required to have undertaken appropriate training before being given access to Trust systems.**

8. EQUALITY

In accordance with the Trust's Equality policy, this policy will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, carer's status, offending background or any other personal characteristic.

9. GOVERNANCE AND REPORTING

Compliance with this policy (and supporting procedures) will be monitored by the Head of Information Governance. An internal audit on the Trust's arrangements in relation to breach reporting will be scheduled in line with the Trust's internal audit strategy.

For assurance, details on FOI activity will be reported to the Quality, Safety and Performance Committee, as well as the Senior Information Risk Owner (SIRO).

The policy will be reviewed every 3 years, unless where it will be affected by major internal or external changes such as:

- Legislation;
- Practice change or change in system/technology; or
- Changing methodology.

10. CONTACTS

A copy of this policy and other policies and procedures referenced are available on the Trust's Intranet site. The Information Governance team is available to provide advice, guidance and support and can be contacted via e-mail on VelindreInformationGovernance@wales.nhs.uk.

11. FURTHER INFORMATION

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

- Information Governance Policy
- Data Protection & Confidentiality Policy
- Freedom of Information Act Policy
- Records Management Policy
- Information Security Policy
- Email and Instant Messaging (EIM) Use Policy

In addition there will be underlying divisional, associated organisational protocols and procedures in place to support Trust wide policies.

Appendix A

Information Governance Risk Table

Domain Impacts on	Insignificant	Minor	Moderate	Major	Catastrophic
	Loss of or unauthorised access to: • A single record containing *special categories of personal data • Less than 5 records containing less *special categories of personal data e.g. demographics. Minimal impact on reputation and little or no expenditure required to recover.	Loss of or unauthorised access to: • Less than 5 records containing *special categories of personal data. • Less than 20 records containing less *special categories of personal data e.g. demographics. Moderate impact on reputation (local press coverage) and costs – expenditure required to recover. Reportable to ICO.	Loss of or unauthorised access to: • Less than 20 records containing *special categories of personal data • Less than 300 records containing less *special categories of personal data e.g. demographics. Major impact on reputation (regional press coverage) and costs – significant expenditure required	Loss of or unauthorised access to: • Less than 200 records containing *special categories of personal data. • Less than 1000 records containing less *special categories of personal data e.g. demographics. Huge impact on reputation and costs –	Loss of or unauthorised access to: • Over 1000 records containing *special categories of personal data • Record(s) containing **highly sensitive personal data. • More than 1000 records containing less *special categories of personal data e.g. demographics.

	Short term embarrassment or harm caused. Complaint possible. Able to deal with using internal mechanisms.	Short term embarrassment or harm caused. Complaints possible. Able to deal with using internal mechanisms.	Short term embarrassment or harm caused. Complaints likely. May involve external regulatory bodies. Potential for ICO fine.	to recover. Reportable to ICO. Short term embarrassment or harm caused. Complaints very likely. Likely to involve external regulatory bodies. Potential for ICO fine.	unable to recover situation. Reportable to ICO. Significant long term, permanent harm, damage or death to patients may occur. Complaints inevitable. Very likely to involve external regulatory bodies. Likelihood of ICO fine.

**special categories of personal data are defined in Data Protection Legislation as 'personal data consisting of information as to data relating to health or sexual orientation information, religion, race or ethnic origin, political opinion, trade union membership, genetic, and biometric data where processed to uniquely identify an individual.

**Highly sensitive personal data includes the NWIS defined list of 'highly sensitive information' which are sexually transmitted diseases, human fertilisation & embryology, HIV & AIDS, termination of pregnancy and gender reassignment and for the purposes of risk assessment also includes other information of a higher sensitivity which, if released, would put individuals at significant risk of harm or distress for example child or adult protection information.

Appendix B

SCORING SYSTEM
FOR CATEGORISING OF PERSONAL DATA BREACHES

The scoring system should be followed step by step. A baseline score will establish the base categorisation level for the incident. This score will then be modified as the following sensitivity factors are applied:

- Low – reduces the base categorisation
- Medium – has no effect on the base categorisation
- High – increases the base categorisation

1. Establish the baseline scale of the incident. If unknown, estimate the maximum potential scale point.

Baseline Scale	
0	Information about less than 10 individuals
1	Information between 11-50 individuals
1	Information between 51-100 individuals
2	Information between 101 – 300 individuals
2	Information between 301 – 500 individuals
2	Information between 501 – 1,000 individuals
3	Information between 1,001 – 5,000 individuals
3	Information between 5,001 – 10,000 individuals
3	Information between 10,001 – 100,000 individuals
3	Information over 100,001+ individuals

2. Identify which sensitivity characteristics may apply and the baseline scale point adjust accordingly.

Low: For each of the following factors reduce the baseline score by 1	
-1 for each	No clinical data at risk
	Limited demographic data at risk e.g. address not included, name not included
	Security controls / difficulty to access data partially mitigates risk
Medium: The following factors have no effect on baseline score	
0	Basic demographic data at risk e.g. equivalent to telephone directory
	Limited clinical information at risk e.g. clinic attendance, ward handover sheet

High: For each of the following factors increase the baseline score by 1	
+1 for each	Detailed clinical information at risk e.g. case notes
	Particularly sensitive information at risk e.g. HIV, STD, Mental Health, Children
	One or more previous incidents of a similar type in the past 12 months

	Failure to securely encrypt mobile technology or other obvious security failing
	Celebrity involved or other newsworthy aspects or media interest
	A complaint has been made to the Information Commissioner
	Individuals affected are likely to suffer significant distress or embarrassment
	Individuals affected have been placed at risk of physical harm
	Individuals affected may suffer significant detriment e.g. financial loss
	Incident has occurred or risk incurring a clinical untoward incident

3. Determine final score. Where adjusted scale indicates the incident is level 2 or above, it should be considered for reporting to the ICO.

Final Score	
1 or less	Considered to be non-reportable to ICO
2 or more	Should be considered for reporting to the ICO

Appendix C

EXAMPLES OF CATEGORISING PERSONAL DATA BREACHES USING SCORING SYSTEM

Example A

Imaging system supplier has been extracting identifiable data in addition to non-identifying performance data. A range of data items including names and some clinical data and images have been transferred to the USA but are being held securely and no data has been disclosed to a third party.		
Baseline scale factor	3 (estimated)	
Sensitivity factors	-1	limited demographic data
	0	limited clinical information
	-1	data held securely
	+1	sensitive images
	+1	data sent to USA deemed newsworthy
Final score level 3 so incident is deemed to be reportable		

Example B

Information about a child and the circumstances of an associated child protection plan has been faxed to the wrong address.		
Baseline scale factor	0	
Sensitivity factors	-1	no clinical data at risk
	0	basic demographic data
	+1	sensitive information
	+1	information may cause distress
Final score level 1 so incident is deemed non-reportable		

Example C

Two diaries containing information relating to the care of 240 midwifery patients were stolen from a nurse's car.		
Baseline scale factor	2	
Sensitivity factors	0	basic demographic data
	0	limited clinical information
Final score level 2 so incident is deemed to be reportable		

Example D

A member of staff took a ward handover sheet home by mistake and disposed of it in a public waste bin where it was found by a member of the public. 19 individual's details were included.		
Baseline scale factor	1	
Sensitivity factors	-1	limited demographic data
	0	limited clinical information
	+1	security failure re disposal of data
Final score level 1 so incident is deemed non-reportable		