Confidentiality Breach Reporting Protocol

Executive Sponsor & Function:

Board Secretary

Document Author:

Information Governance Manager

Approved by:

Executive Team

Approval Date:

29 January 2020

Date of Equality Impact Assessment:

14/03/2019

Equality Impact Assessment Outcome:
This policy has been screened for relevance to equality. No potential negative impact has been identified so a full equality impact assessment is not required.

Review Date:

January 2023

Version: v1

TABLE OF CONTENTS

1. DOCUMENT HISTORY

1.1 Revision History

Date	Version	Author	Revision Summary
8/1/2019	V0.1	Tim Knifton	Initial draft with updates for HEIW

1.2 Reviewers

This document requires the following reviews:

Date	Version	Name	Position
	Final	Dafydd Bebb	Board Secretary

1.3 Authorisation

Signing of this document indicates acceptance of its contents.

Author's Name: Tim Knifton	
Role:	
Signature:	Date:

Approver's Name: Dafydd Bebb	
Role:	
Signature:	Date:

1.4 Document Location

Type	Location
Electronic	Corporate Policy Library
Hard Copy	

EXECUTIVE SUMMARY
Confidentiality breach reporting protocol

Overview:	The Confidentiality breach reporting protocol sets out a set of principles which staff members must adhere to when reporting suspected breaches of confidentiality, affirming Health Education and Improvement Wales' (HEIW) organisational commitment to robust Information Governance Practices. This protocol sets out the intent of the organisation (and its staff) in ensuring that suspected (or alleged) breaches of confidentiality are effectively reported to the appropriate parties for action and recorded for onward investigation.
Who is the protocol Intended for:	All Health Education Improvement Wales (HEIW) staff including everyone working for or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts.
Key Messages included within the protocol:	To discuss the attached Confidentiality Breach reporting protocol and the organisations commitment to comply with requirements while raising staff awareness of responsible confidential data use.
	This protocol covers the reporting and recording mechanism that must be followed when reporting alleged, suspected or confirmed confidentiality breaches.
PLEASE NOTE THIS IS ONLY A SUMMARY OF THE PROTOCOL AND SHOULD BE READ IN CONJUNCTION WITH THE FOLLOWING FULL DOCUMENT	

2.0 Introduction

This protocol affirms Health Education and Improvement Wales' (further known in this protocol as HEIW) commitment to ensuring that correct use of confidential information is observed at all times and any suspected breaches of confidential data (defined as personal or sensitive personal data, and commercially sensitive data) is acted upon.

There are instances that could be identified as being a suspected breach of confidentiality that will require further investigation. Those potential breaches should be initially investigated by the appropriate line manager and those that are confirmed as a suspected incident are reported accordingly so that they can be investigated thoroughly.

This protocol provides a mechanism for reporting suspected confidentiality breaches that have been identified in order to effectively record them for onward action by the appropriate manager or nominated contact in co-operation with the HEIW Information Governance Manager.

3.0 Purpose and scope of this protocol

The purpose of this protocol is to put in place a standardised management approach throughout HEIW and its respective departments 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.

The protocol applies to everyone working for or engaged by HEIW including part time workers, temporary and agency workers and those holding honorary contracts.

4.0 Equality Impact Assessment

An Equality Impact Assessment has been undertaken that involved assessing the likely or actual effects of decisions, policies or services on people in respect of age, disability, gender and racial equality, pregnancy and maternity, race, religion or belief, sex and sexual orientation. It helps us to make sure the needs of people are taken into account when we develop and implement a new protocol, policy or service or when we make a change to a current policy, protocol or service.

5.0 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.

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

- Accessing unauthorised computer systems fraudulently or using/sharing other employee 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 the service delivery.
- Misdirection of an email.
- 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, cd's, memory sticks, mobiles, iPads, etc.

6.0 Reporting Arrangements

Whenever a suspected personal data breach incident has occurred it is imperative staff report the incident to their line manager and follow the organisation's Incident Reporting and Investigation Policy (including Serious Incidents) recording as much detail as possible of the incident into HEIW's Incident Reporting System.

More serious personal data breach incidents must be reported directly to key staff e.g. Data Protection Officer (DPO), Senior Information Risk Owner (SIRO), Caldicott Guardian and the Information Governance (IG) Manager, as early notification and preparation is key to dealing with management and investigation of reported personal data breach incidents.

6.1 Personal Data Breach Investigation

The objective of any breach investigation is to identify what actions HEIW needs 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).

Key to preventing any recurrence is to ensure that HEIW learns from reported incidents, and where applicable share lessons learnt, and consider any trends and identify areas for improvement.

6.2 Incident Classifications

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

Organisations must have appropriate means in place to regularly review personal data breach incidents and where necessary cascaded within the appropriate organisational forums and Executive Team.

6.3 Notifying individuals or other parties

Depending on the seriousness of the personal data breach, HEIW may be required to inform some or all of the following:

- The individuals concerned;
- The Information Commissioner's Office (ICO);
- HEIW Senior Management (including the SIRO and Chief Executive);
- HEIW Caldicott Guardian;
- HEIW Data Protection Officer (DPO);
- Welsh Government;
- Regulatory bodies (i.e. GMC, LMC, etc);

- Associated organisations i.e. NHS Wales Health Boards and Trusts;
- The Police.

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

6.3.1 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, HEIW must ensure that no further confidential data is disclosed, i.e. sending notifications to the wrong home or email addresses.

6.3.2 The Information Commissioners Office (ICO)

The HEIW Information Governance Manager in conjunction with discussions made with the SIRO and DPO, will inform the ICO if the breach involves personal data and to consider if the breach:

- has been assessed in line with the ICO data breach reporting guidelines;
- means whether a statement is to be made to the Welsh Government and/or a media announcement is to be made; or
- 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, 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 organisation becoming aware of the personal data breach. Where notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

7. Responsibilities

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

7.1 Managerial Accountability and Responsibility

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

HEIW has a legal obligation to appoint a Data Protection Officer, whose role will be 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.

Directors of departments within HEIW are responsible for ensuring the protocol is implemented within their areas, and must ensure:

- That their organisation complies with this protocol;
- All staff and contractors are aware of the requirements incumbent upon them;
- Delegating the day-to-day responsibility to information governance leads defined by departments within HEIW as appropriate to their needs.

HEIW has a dedicated Information Governance lead. This role 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 the respective departments on compliance with the legislation.

All staff are required to comply with this protocol and respect the personal data and privacy of others in their day-to-day working practice. Staff must ensure that 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 protocol and any employee who is found to compromise security or confidentiality of HEIW, including its employees, service users or contractors may be subject to the HEIW Disciplinary Policy.

8. Legislation/Standards

This protocol 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:

- Data Protection Legislation
- The General Data Protection Regulation
- Common Law - Duty of Confidence
- Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000

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

- Caldicott
- Information Security ISO27001
- Information Commissioner’s Codes of Practice

9. Staff Training Needs Analysis for Information Governance training

Currently, staff training needs analysis for Information Governance is being determined by HEIW Information Governance Manager.

Arrangements are in place to ensure that all staff identified as “high risk” working with identifiable information within HEIW will receive bi-annual, Information Governance face to

face training that will give those staff the appreciation of the confidentiality of the data that the organisation holds and their responsibilities for securing it. This is above and beyond the eLearning Information Governance core skills training that is completed online.

Any details of training sessions undertaken will be noted on the staff members' education and training record through the Electronic Staff Record (ESR) system.

10. Monitoring

Compliance with this protocol will be monitored by the Information Governance Manager and Executive department within HEIW. The protocol will be reviewed every 2 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.

11. Contacts

For further advice and/or assistance on how to ensure compliance with this protocol or to request further information, then please contact:

HEIW's Information Governance Manager

12. Legislation and Guidance

Staff are advised to read this document in conjunction with HEIW's other relevant policies:

- Information Governance protocol
- Data Protection & Confidentiality protocol
- Information Security protocol
- Information Governance protocol
- All Wales Internet and Email protocol
- Taking information offsite protocol
- Disciplinary Policy

Other references

Privacy and Electronic Communications Regulations 2003
UK Data Protection Bill
General Data Protection Regulation
The Caldicott Report 2013
Computer Misuse Act 1990
Copyrights, Designs & Patents Act 1988
Human Rights Act 1998
Freedom of Information Act 2000
DoH: Records Management: Code of Practice June 2006
Information Governance Assurance Programme Guidance 2008-9
Data Protection (Processing of Sensitive Personal Data) Order2000
Fraud Act 2006
Professional Codes of Conduct

Appendix A – Information Governance risk table

Domain Impacts on	Insignificant	Minor	Moderate	Major	Catastrophic
	Loss of or unauthorised access to: • A single record containing *sensitive personal data • Less than 5 records containing less sensitive personal data e.g. demographics.	Loss of or unauthorised access to: • Less than 5 records containing *sensitive personal data. • Less than 20 records containing less *sensitive 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 20 records containing *sensitive personal data. • Less than 300 records containing less sensitive 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 200 records containing *sensitive personal data. • Less than 1000 records containing less sensitive personal data e.g. demographics. Major impact on reputation (regional press coverage) and costs – significant expenditure required to recover. Reportable to ICO.	Loss of or unauthorised access to: • Over 1000 records containing sensitive personal data • Record(s) containing **highly sensitive personal data. • More than 1000 records containing less sensitive personal data e.g. demographics. Huge impact on reputation and costs – unable to recover situation. Reportable to ICO.

Domain Impacts on	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
	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.	Short term embarrassment or harm caused. Complaints very likely. Likely to involve external regulatory bodies. Potential for ICO fine.	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.

*Sensitive personal data is defined in Data Protection Legislation as 'personal data consisting of information as to... his physical or mental health or condition', which would include a health record or other information about an individual's health.

**Highly sensitive personal data includes the 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		