GIG CYMRU NHS WALES | Iechyd Cyhoeddus Cymru Public Health Wales	**Reference Number:** PHW 60/TP01 **Version Number:** 1 **Date of Next review:** 9 June 2018

National Intelligent Integrated Audit Solution

Introduction and Aim

This procedure has been developed to inform employees about the process relating to the access of service user, patient and staff information and to enable Managers to respond to and deal effectively with notifications that are raised from the National Intelligent Integrated Audit Solution (NIIAS).

Linked Policies, Procedures and Written Control Documents

Confidentiality Code of Practice for Health and Social Care in Wales
Information Governance Policy (PHW13)
Handling Requests for Information Procedure (PHW 22)
Disciplinary Policy and Procedure
Code of Conduct (Disciplinary Rules and Standards of Behaviour)

Scope

This procedure applies to all employees of Public Health Wales .

Equality and Health Impact Assessment	This Procedure applies across the organisation. There is no evidence to suggest any disproportionate or negative impact on any specific group of staff on grounds of their protected characteristics.
Approved by	Information Governance Working Group
Approval Date	9 June 2017
Review Date	9 June 2018
Date of Publication:	19 June 2017
Accountable Executive Director/Director	Rhiannon Beaumont-Wood, Executive Director Quality, Nursing and Allied Healthcare Professionals.
Author	John Lawson, Chief Risk Officer

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or Corporate Governance.

Summary of reviews/amendments				
Version number	**Date of Review**	**Date of Approval**	**Date published**	**Summary of Amendments**

1 Introduction

The security of service user, patient or staff information within Health Boards and Trusts has been given a high profile in recent years and is taken extremely seriously by the organisation. The Information Commissioner's Office (ICO) now has increased powers, including the power to penalise organisations up to £500,000 for serious breaches. As well as the financial implication there is also the impact that any publicised breach will have on the organisation's reputation.

Any breaches of this procedure may be investigated as a disciplinary matter under the appropriate Policy.

To assist in continuing to keep personal information secure and confidential, NHS Wales Informatics Service (NWIS) has provided NHS Wales with Privacy Breach Detection software, called National Intelligent Integrated Audit Solution (NIIAS).

NIIAS will be linked to clinical systems and can be used to analyse activity on these systems and report on instances where potentially inappropriate access has occurred.

Inappropriate behaviour is where system users look up records which the user has no valid work reason to view and includes records of:

- Colleagues
- Family members
- Neighbours
- Themselves
- Any other record which the user has no valid work reason to view

Looking up the above records for 'practice' or training is also an inappropriate use.

Training environments can be accessed in:

- ASIMS
- BSIMS
- Canisc
- LIMS
- WDS

The introduction of NIIAS does not change anything about the way Public Health Wales staff are expected to work, neither does it alter the terms and conditions for staff or the disciplinary process which

may arise from a breach. NIIAS simply automates the auditing and alerting system which allows us to ensure that we remain compliant with legislation. It has always been a condition of employment that access to personal information is on a strict need-to-know basis. All staff are required to comply withThe Confidentiality Code of Practice for Health and Social Care in Wales or with the relevant code of practice relating to their professional role.
http://www.wales.nhs.uk/nhswalescodeofconductandcodeofpractice

NIIAS is an additional means by which we can assure our service users, staff, the Board and the Information Commissioner that the information we hold is handled correctly and in accordance with the law.

If a member of staff wishes to view their own health records, or those of a dependent relative, they must follow the same process as any member of the public by following the Subject Access Request process as stipulated in the Data Protection Act 1998. Guidance on this process can be obtained from the Information Governance key policies and documents page on the intranet:

Handling Requests for Information Procedure

The introduction of NIIAS does not alter any of the policies of Public Health Wales or existing laws regarding access to service users' or patients' health records. NIIAS simply identifies and highlights instances where staff privileges are suspected of being abused.

This document is intended to offer general guidance in the event a NIIAS notification is received related to an employee. The guidance will be applied consistently, regardless of the position or designation of the employees involved. Compliance with the Data Protection Act is a legal requirement and Public Health Wales must be able to demonstrate that non-compliance is dealt with appropriately.

2 Roles and responsibilities

Employees

Employees are required to adhere to the organisation's policies on information governance and these guidelines.

Employees will only access service user, patient or staff information for the purpose of their role. Although employees may have the ability to access personal information because of their role, it does not automatically grant them the right to do so.

Managers

Managers should ensure that employees are fully aware of their responsibilities in respect of service user, patient or staff information and that personal information should only be viewed if there is a legitimate clinical or administrative reason to do so. Managers are also responsible for ensuring that their staff are up to date on Information Governance mandatory training

Information Governance

The Information Governance department will notify appropriate managers when a breach has taken place.

The Information Governance Department will provide advice and guidance on the process.

People and Organisational Development

The People and Organisational Development department will provide advice and guidance to managers and employees in respect of any potential breach of the guidelines.

3 Procedure

3.1 Following a notification from NIIAS identifying a suspected inappropriate access of information, an email notification will be issued to the appropriate manager by a member of the Information Governance team.

3.2 The manager reviews whether there is a legitimate clinical or administrative reason for the employee to have accessed the records. This should be commenced within five working days of receipt of the email.

3.3 Once the manager has identified the reason for the access of the information and whether this has been done for a legitimate clinical or administrative reason, they need to inform the Information Governance department by responding to the initial notification email confirming that the access was legitimate or not. The notification will remain active until Information Governance receives the outcome.

3.4 If it is identified that there was no inappropriate access then no further action will be taken nor will the staff member necessarily be informed.

3.5 If it is identified that the access may be inappropriate then managers should contact the People and OD department and any investigation carried out in line with Public Health Wales Disciplinary Policy. Any action taken will also be in line with the Disciplinary Policy.

4 Training requirements

All employees will be made aware of the procedure upon commencement with Public Health Wales and copies can also be viewed on the Public Health Wales intranet.

All Public Health Wales employees are required to undertake Information Governance training every 2 years.

Investigation training is carried out by the People and OD department and managers responsible for investigating NIIAS notifications should ensure they arrange to attend this training.

5 Monitoring compliance

The Chief Risk Officer will monitor this procedure to ensure it is compliant with current legislation and to ensure it is effectively implemented.

6 Appendices

Appendix 1 - Examples of potential NIIAS breaches.

Examples of potential staff breach as identified by NIIAS	Potential (inappropriate) reasons for breach
Staff member accesses their own health records	• To check if the information stored is accurate. • To update a record i.e. Change of Address. • To check date and time of upcoming appointment. • To access lab results or check a diagnosis.
Staff member accesses someone else's health records e.g. child or other family member, neighbour, colleague, celebrity etc	• To check if the information stored is accurate. • To update a record i.e. Change of Address. • To check date and time of upcoming appointment. • To access lab results or check a diagnosis. • At the request of a third party to confirm information, appointment or results. • Checking for birthday, address, phone number (for personal reasons). • Checking to find out if a pregnant colleague has had their baby. • Practising on a system using familiar names.
Staff member shares information only known as a result of their employment, or accesses someone else's personal information and shares it with a third party	• At the request of the third party – e.g. confirming that someone is pregnant, or received treatment for an overdose. • Checking a colleagues record to find out why they are absent from work. • Checking the record of a well known person and sharing information with a third party.