UNAUTHORISED ACCESS TO PATIENT RECORDS - REPORTING AND ESCALATION PROCEDURE

Procedure information

Procedure number: 773

Classification:
Corporate

Supersedes:
N/A

Version number:
1

Date of Equality Impact Assessment:
12/07/2022

Approval information

Approved by:
Sustainable Resources Committee

Date of approval:
27/06/2023
Date made active:
28/06/2023
Review date:
27/06/2026

Summary of document:
This document includes the correct procedure for the use of the National Integrated Intelligence Audit Solution (NIIAS) to identify potentially inappropriate access to clinical records and how to escalate this through an agreed process.

Scope:
All staff with access to electronic clinical systems will be affected by the introduction of NIIAS. Staff within the Health Board have been fully briefed as to what this system will deliver through a robust communications plan, Information Governance training sessions and discussions at the relevant forums (including Staff Partnership Forum). Communication reminders are sent to staff on a regular basis to remind them of their responsibilities in relation to accessing patient records and respecting patient privacy and confidentiality.

To be read in conjunction with:
[320 – Acceptable Use of IT Policy] – opens in a new tab
[172 – Confidentiality Policy]– opens in a new tab
[836 – All Wales Information Governance Policy] – opens in a new tab
[837 – All Wales Information Security Policy] – opens in a new tab
[995 - All Wales Respect and Resolution Policy] – opens in a new tab
[201 - All Wales Disciplinary Policy and Procedure] – opens in a new tab
[435 - All Wales NHS Staff to Raise Concerns Procedure (Whistleblowing)] – opens in a new tab
[488 - All Wales Upholding Professional Standards in Wales (Medical & Dental Staff) Policy] – opens in a new tab

Patient information:
Include links to Patient Information Library

Owning group:
Information Governance Sub Committee
08/04/2023

Executive Director job title:
Huw Thomas , Director of Finance

Reviews and updates:
1.0 New Procedure 27.6.23

Keywords
NIIAS, Audit, Information Governance, Unauthorised Access

Glossary of terms

Term	Definition
Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.
Data Protection Legislation	Data protection legislation is about the rights and freedoms of living individuals and in particular their right to privacy in respect of their personal data. It stipulates that those who record and use any personal data must be open, clear and transparent about why personal data is being collected, and how the data is going to be used, stored and shared.
NIIAS	National Integrated Intelligent Audit Solution
Personal Data	Personal Data is information which relates to a living individual who can be identified from the information itself or by linking it with other information – for example a person's name and address, an online profile, a member of staff's HR record or records relating to individual's such as patients or service users.
Personal Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised

	disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.
Senior Information Risk Owner (SIRO)	An Executive Director or member of the Senior Management Board with overall responsibility for information risk across the Health Board.
Special Category Data	Special category data means personal data consisting of information as to: - Genetic and biometric data - Political opinions - Religious or other beliefs - Trade union membership - Physical or mental health/condition - Sexual life And although not specifically described as special category data, this information requires the same treatment: - The commission or alleged commission of any offence - Any proceedings for any offence committed/alleged to have been committed, the disposal of such proceedings or the sentence of such proceedings
Unauthorised Access	Access to information that is not part of your work duties. Access to a patients record where the patient is not under your care.

Contents

Scope

All staff with access to electronic clinical systems will be affected by the introduction of NIIAS. Staff within the Health Board have been fully briefed as to what this system will deliver through a robust communications plan, Information Governance training sessions and discussions at the relevant forums (including Staff Partnership Forum). Communication reminders are sent to staff on a regular basis to remind them of their responsibilities in relation to accessing patient records and respecting patient privacy and confidentiality.

Aim

The aim of this document is to:

- ensure appropriate and relevant access to Patient Identifiable Information (PII).
- ensure that all staff understand their responsibilities when accessing patient records.
- educate staff on the process Information Governance will take on any identified inappropriate access to information.
- ensure the Health Board has taken all steps possible to educate staff to prevent any future breaches of confidentiality.

Objectives

The aim of this document will be achieved by the following objectives:

- Identify any potential inappropriate access to PII in line with the principles of the current Data Protection Legislation and confidentiality and privacy laws to ensure that patient information is handled by staff members fully respecting the privacy rights of each individual patient.
- Escalate any potential Personal Data Beaches to the Information Governance team so that action can be taken.
- Where a case has to be answered, inform the Workforce Department to follow the processes outlined within this procedure and which may result in action being taken in line with the Health Board's Disciplinary Policy and Procedure – opens in a new tab.

Introduction

The National Intelligent Integrated Audit Solution (NIIAS) will take the audit trail from electronic clinical systems, e.g. Welsh Patient Administration System (WPAS), Laboratory Information Management System (LIMS), the Welsh Clinical Portal (WCP) and cross match against both an employee record in the Electronic Staff Record (ESR) and the Health Board's national directory (Cymru). NIIAS will then report on any unauthorised access to person identifiable information (PII) against the domains outlined in section 2.1.

Procedure

The Procedures follow several steps to identify and escalate potential personal data breaches:

Definition of the 8 domains

Breaches have been defined on a National level and fall into the following 8 domains.

Term	Definition	Comment
Own Care Record	A user has accessed their own patient records.	Identification of Patient IDs for the staff member through ESR-MPI triangulation.
Family Care Record	A User has accessed the record of a Patient who has the same surname and postcode as the User.	Family classified as matching same surname + postcode through ESR-MPI triangulation.
Staff Member Record	A User has accessed the record of a Patient who has a matching employee record in ESR.	
Living in the Same Vicinity	A User has accessed the record of a Patient who lives very close to the User. In rural areas this distance is 0.5 miles, in urban areas this distance is 0.1 miles.	Identification of distance between User and Patient postcodes through ESR-MPI triangulation.
Person of Interest	A User has accessed the record of a Patient who has been flagged by the HBs as being a “person of interest”.	This Patient is flagged locally using their NHS number.
Patients with the Same Surname	A User has accessed three Patients in the space of 1 day who share the same surname.	The 15 most common surnames in Wales have been excluded (Davies, Edwards, Evans, Griffiths, Hughes, James, Jenkins, Jones, Lewis, Morgan, Rees, Roberts, Smith, Thomas, and Williams).
Historic Record	A User has accessed patient records that are older than 1 year without first accessing a more recent record for that same Patient within the last 45 days.	Users with Clinical Job Roles assigned in ESR are excluded.
Deceased Patient	A User has accessed the records of a deceased Patient who has been deceased for more than 60 days.	Identification of deceased patient through MPI.

The Health Board is currently enforcing the following domains:

- Access to Own Record;
- Access to Family Record;
- Access to Persons of Interest;
- Access to Deceased patient's records; and
- Access to Staff Members Records.

Process for managing Access to Own Record: First time accessed by staff member (See Appendix 1 for flow chart)

The Information Governance team will produce a daily report that will identify any staff accesses to own record. Any staff member identified through the report will be sent an e-mail with an attached letter from the Information Governance Team outlining the details of the access. The attached letter will advise staff that they need to share a copy of the letter with their line manager within 5 working days, and attend one of the Information Governance Awareness Training sessions. Individuals are advised that attendance at the training session will be recorded on their ESR record.

Line Managers are then requested to confirm receipt of the letter to the Information Governance Team within 10 working days by completing the attached FORM 1 and confirming which of the Information Governance Awareness training sessions the individual will attend.

Staff will then book via ESR or directly with IG onto a virtual training session of their choosing.

Following completion of the training, any further attempts by a staff member to access their Own Record within a two-year period will be dealt with formally through the NIIAS procedure for further access to own record (see point below).

NB: If at any point during the analysis of the NIIAS report the Information Governance Team, Executive Lead or Manager suspects there has been serious malpractice carried out by an employee a full investigation can be undertaken.

If a member of staff fails to respond to the Information Governance team, manager details are requested via Workforce.

Process for managing Access to Own Record: Further access by staff member (See Appendix 2 for flow chart)

The line manager for the staff in question will be contacted and asked to complete an 'Initial Assessment of Facts Form'. This will be returned to the Information Governance Team within 10 working days.

If it is not possible to identify the line manager for the staff member in question, the process outlined in the point above will be followed to make initial contact with the staff member and to request details of their line manager.

The Information Governance Team will review the returned 'Initial Assessment of Facts Form'. If the access is deemed as appropriate by the line manager (i.e. there is a legitimate work reason for the staff member accessing the record) and this is confirmed and agreed by the Information Governance team, the case will be closed on the NIIAS tracker and no further action taken.

If the access was inappropriate, the Information Governance Team will send details of the access and the outcome of the returned 'Initial Assessments of Facts Form' and investigation through to the identified link in the Workforce team to initiate the procedure as detailed in the All Wales Disciplinary Policy and Procedure document – opens in a new tab.

The Workforce team will liaise with the line manager to agree any further action required in relation to the staff member.

The Information Governance Team will provide any appropriate NIIAS reports as requested by the Workforce team.

Process for managing access to Family Record, Staff Record, Persons of Interest and Deceased patient's records. (See Appendix 3 for flow chart)

The Information Governance team will produce a report daily that will identify any staff accesses to the records above.

The individual staff member will be sent an e-mail with an attached basic letter advising them they have been identified through the NIIAS system as potentially having accessed a record without authorisation to do so. Staff will be asked to enter details of their line manager onto the contact letter and return this to the Information Governance team within 5 working days.

The Information Governance team will then contact the line manager directly with full details of the breach and ask that they complete an 'Initial Assessment of Facts Form' to identify whether the access is appropriate or not in relation to their staff member. This form will then be returned to the Information Governance team within 10 working days.

Appropriate access to records of Family Member, Staff Record, Persons of Interest and Deceased patient's records.

If the breach is deemed as appropriate by the line manager (i.e. there is a legitimate work reason for the staff member accessing the record) and this is confirmed and agreed by the Information Governance team, the case will be closed on the NIIAS tracker and no further action taken.

Inappropriate access to record of Family Member, Staff Record, Persons of Interest and Deceased patient's records.

The line manager will be required to conduct a formal meeting with the staff member to advise them that their access to the record is not appropriate, remind them of the NIIAS procedure and the Health Board's Confidentiality Policy – opens in a new tab. The line manager may wish to link in with their HR advisor within the Workforce team to assist with this process if further support is required.

The IG Team will run a full NIIAS check report against the individual to ensure there are no wider concerns about the individual's access to patient records.

The staff member will be required to attend an Information Governance training session within three months. The NIIAS tracker will be updated once the staff member has completed their IG training and the IG Team have completed their report. If no further inappropriate access to records takes place and no wider concerns are identified, then no further action will be taken and the case will be considered for closure.

If the access relates to more than a single record access or, if there are wider concerns confirmed or noticed about the individual's access to records, the Information Governance Team will commence the procedure for Managing Information Governance Incidents. This will be run alongside any on-going disciplinary/Workforce investigation. The Information Governance and Workforce teams will share information from their on-going investigations where it is felt appropriate to do so.

As part of the Managing Information Governance Incidents Procedure, the Information Governance Team will report the breach to the Caldicott Guardian and Senior Information Risk Owner who may decide to immediately suspend the staff member's access to patient records whilst the investigation is on-going. The Information Governance team will also need to determine if the breach is reportable to the Information Commissioner Office, this is in accordance with the Health Boards statutory obligations to report personal data breaches.

Once the investigation has concluded the Information Governance team will be informed by the Workforce link

NB: If at any point during the analysis of the NIIAS report the Information Governance team, Executive Lead or Manager suspect there has been serious malpractice carried out by an employee i.e. evidence that a large number of records have been accessed or multiple family members etc, this should be reported immediately to the Head of Information Governance and the Director of Digital Services.

Escalation process for all non-responses from staff and managers

If an individual member or line manager do not respond to requests for information from the Information Governance team within the agreed time-scales at any stage of the NIIAS process, the following action will be taken:

- An initial chaser e-mail will be sent by the Information Governance Team requesting a response within 5 working days.
- If no response, then the Workforce will be contacted for the employees managers details. If the manager fails to respond their line manager will be contacted.
- If no response received details will be sent to the relevant Executive Director who will contact the line manager requesting a response within 10 working days be sent to the Information Governance team.

Escalation process for not attending a booked Information Governance training session (without giving prior notice to the IG Team)

- An e-mail will be sent to the individual's line manager advising their staff member did not attend the IG training session. The line manager will be requested to remind the individual to book onto another IG training session and to respond within 5 working days.
- If no response then a second chaser e-mail will be sent requesting a response within a further 5 working days.
- If the individual does not attend the re-booked IG training session that their line manager has confirmed, they will be referred to their Executive Director with a request that they attend the next training session available, and their line manager will be copied into this e-mail.
- If the line manager does not respond to any requests to re-book their staff member onto a future session by the IG team then they will be referred to their Executive Director and a response will formally be requested.

Choose Pharmacy Application

The Choose Pharmacy application supports the delivery of a number of NHS community pharmacy services and enables access to NHS patient record systems including the Welsh Demographic Service and the Welsh GP Record.

The Health Board will be responsible for monitoring community pharmacy staff's access to patient data through the above application via the NIIAS monitoring tool.

The NIIAS system provides a report of potential breaches, this is then analysed by the Information Governance team on a twice weekly basis.

The Information Governance Team will then e-mail a report of any potential breaches to the Primary Care Manager (Community Pharmacy).

The Primary Care Manager will then contact the relevant pharmacy and ask that the following process is completed:

Pharmacy staff accessing their own record on one occasion (See Appendix 4 for flow chart)

The Pharmacist must issue a warning email for staff members accessing their own record on the first occasion. They must confirm that this action has been completed to the Primary Care Manager. The Primary Care Manager will then inform the Information Governance Team that this action has been taken.

Where the access has been made by the pharmacy superintendent/pharmacy owner, the Primary Care Manager will send the warning email.

Pharmacy staff accessing their own record on more than one occasion or potentially accessing another person's record inappropriately (See Appendix 5 for flow chart)

The Primary Care Manager will request that the Pharmacist undertake an initial assessment using the Potential Access Breach – Initial Assessment Form to establish whether there is a legitimate clinical or administrative reason for the staff member to have accessed the record(s) for second access to own record or all other potential breaches.

The potential breach will be communicated to the superintendent pharmacist for the community pharmacy at which the breach occurred. The superintendent will provide the Primary Care Manager with the name of the person who will undertake the initial assessment within 5 days.

The initial assessment must be undertaken within 10 working days from a date agreed between the superintendent/owner and the Health Board.

The outcome of the initial assessment should be communicated to the Primary Care Manager via the Potential Access Breach – Initial Assessment Form.

Where the assessment concludes that no further action is necessary the Primary Care Manager will confirm they are satisfied with this decision. The Primary Care Manager will inform the Information Governance Team that no further action is required.

Where the assessment indicates the need for a full investigation – this should be completed in line with the pharmacy Information Governance policy for the management of Information Governance incidents. Access to the Choose Pharmacy application may be removed for the duration of the investigation. The outcome of the investigation will be reported to the Primary Care Manager who will inform the Information Governance Team that the record can be closed.

Any further general learning or training identified following the investigation will be agreed between the Primary Care Manager and the Information Governance team and progress monitored through the Information Governance tracker.

If the inappropriate access is carried out by the Pharmacy Owner/superintendent pharmacist then the Primary Care Manager will appoint an appropriate individual within the Health Board to carry out a full investigation.

Training

All staff will be required to have appropriate Information Governance training, additional training can be requested by individuals or line managers. Training will be provided in several formats to accommodate all learning styles and the requirements of staff and The Health Board.

Implementation

Extensive communications exercises have been undertaken to ensure all staff groups are aware of NIIAS and the implications of any breaches identified. This will be further supported through Information Governance communications via Globals / Newsletters / IG Awareness on Intranet.

Review

This Procedure will be reviewed in line with the further roll out and enforcement of the policy rules, or sooner, as required.

References

Information Commissioner Office https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Appendix 1 – Process for managing Access to Own Record: First access by staff member

Own record access picked up by NIIAS and IG Team.

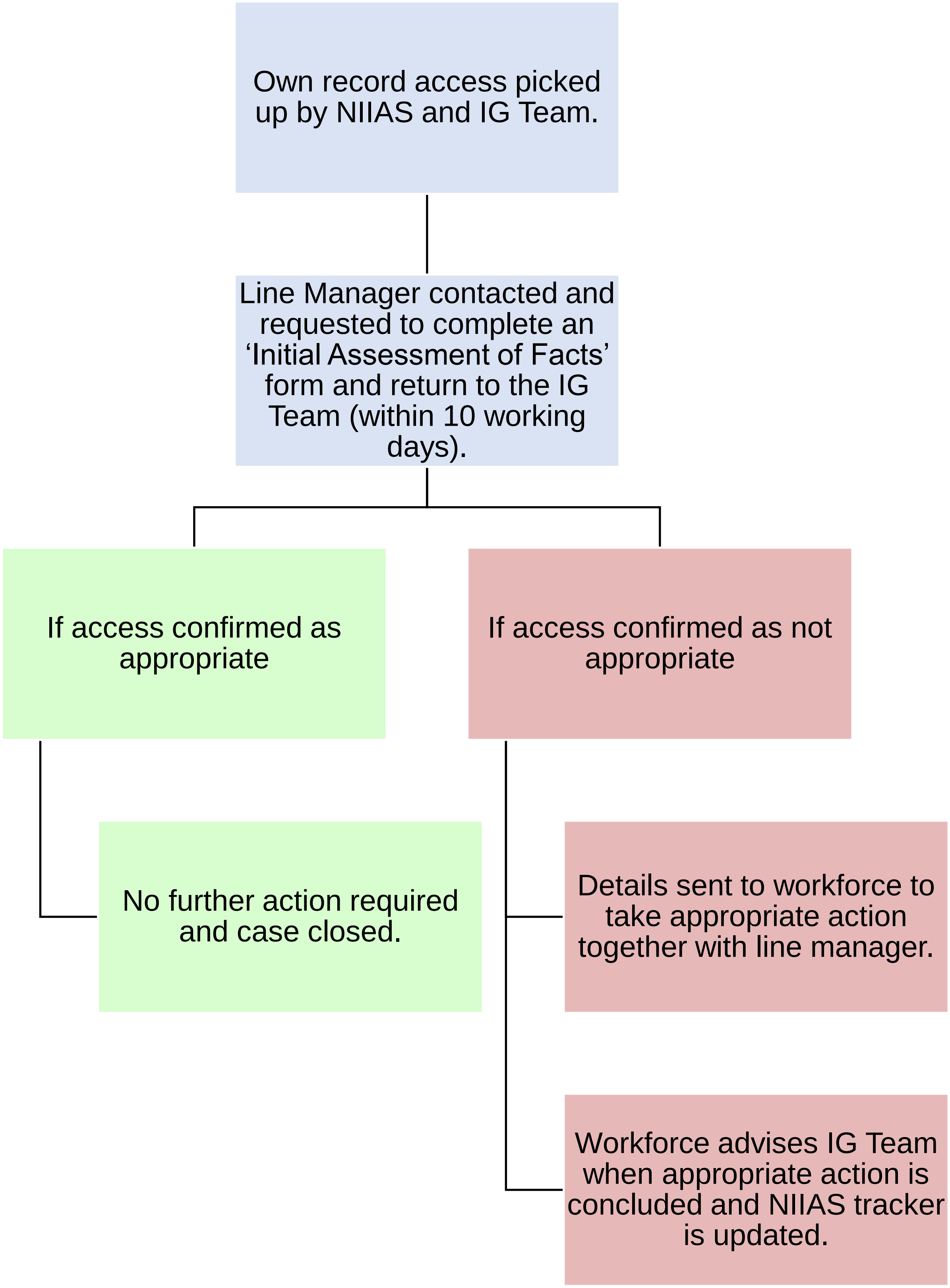
Letter to staff member advising NIIAS has identified a potential breach and requesting they forward letter to line manager (within 5 working days).

Line Manager confirms receipt of letter to IG Team (within 10 working days) and advises the IG training session that the staff member will be attending.

Staff member books training on ESR and attends IG training session

If no further inappropriate access to records are reported then the case is closed.

Appendix 2 – Process for managing Access to Own Record: Further access by staff member



Appendix 3 - Process for managing access to Family Record, Staff Record, Persons of Interest and Deceased patient's records.

Family record access picked up by NIIAS tracker and IG Team

Letter to staff member advising NIIAS has identified a potential breach and asking for line manager details. (To be returned to IG Team within 5 working days).

Letter to line manager providing details of the breach and asking to confirm if access is for a legitimate work purpose with the staff member.

If access confirmed as not appropriate

Single access no wider concerns

Staff member attends formal NIIAS training (within 2 months).

Manager undertakes Formal Counselling with staff member with HR involvement if required

If wider concerns identified about the staff member's access to records

IG team run full NIIAS report against individual's access to records. IG Team to instigate Managing Information Governance Incidents Procedure.

Manager and Workforce to assess the access and to pursue formally in accordance with appropriate procedures.

If access confirmed as appropriate

If all steps completed and no wider concerns

IG Team confirm outcome and update tracker as closed

Appendix 4: Pharmacy staff accessing their own record on one occasion

Own record access picked up by NIIAS tracker and IG Team

↓

IG Team will e-mail a copy of the report to the Primary Care Manager (Community Pharmacy).

↓

Primary Care Manager will contact relevant Pharmacist and request that an initial warning e-mail is sent to the staff member (within 5 working days).

↓

Pharmacist will confirm to Primary Care Manager once this action has been taken.

↓

If no further inappropriate access reported then the case will be closed on the NIIAS tracker.

Appendix 5: Pharmacy staff accessing their own record on more than one occasion or potentially accessing another person's record inappropriately