DIGITAL HEALTH AND CARE WALES
CHOOSE PHARMACY NIIAS PROCEDURE

Document Version	V2.1

Status	Approved

Document author:	Lydia Hutton
Approved by	Approvers' Panel
Date approved:	26/10/2021
Review date:	Sept 2024

TŶ GLAN-YR-AFON 21 Heol Ddwyreiniol Y Bont-Faen, Caerdydd CF11 9AD

TŶ GLAN-YR-AFON 21 Cowbridge Road East, Cardiff CF11 9AD

TABLE OF CONTENTS

1. DOCUMENT HISTORY

1.2 REVISION HISTORY

Date	Version	Author	Revision Summary
09/2016	1.0	Emma Williams	First version
09/2018	1.1	Emma Williams	No changes to version – extended for period of 2 years
09/2021	2.0	Emma Williams	Updated document and circulated with reviewers
30/09/2021	2.1	Lydia Hutton	Template updated to DHCW, recorded approval dates from governing bodies/review panels

1.3 REVIEWERS

This document requires the following reviews:

Date	Version	Reviewer panel
20/06/2021	V2.0	Community Pharmacy Wales (CPW) Board Members
October 2020	V2.0	NHS Wales Health Board leads responsible for monitoring Choose Pharmacy NIIAS notifications
26/10/2021	V2.1	DHCW Information Governance team

1.4 APPROVERS

This document requires the following approvers:

Date	Version	Reviewer panel
20/06/2021	V2.0	Community Pharmacy Wales Board
27/09/2021	V2.0	All Wales Chief Pharmacists' Group
26/10/2021	V2.1	DHCW NIIAS Management Board

1.5 AUTHORISATION

Signing of this document indicates acceptance of its contents.

Author's Name:	Emma Williams
Role:	Choose Pharmacy Clinical Lead
Signature:	

1.6 DOCUMENT LOCATION

Type	Location
Electronic	Microsoft Teams – Choose Pharmacy Project – 6.0 Assurance and I.G.

2. AUDITING & ESCALLATION PROCESS

Date to be reviewed:	Sept 2024	**No of pages:**	
Author(s):		**Author(s) title:**	
Responsible dept / director:	Information Governance NHS Community Pharmacy Contract manager		
Approved by:			
Date approved:			
Date of review:	3 years from date of approval or sooner in the event of significant legislation or service change		

Date EQIA completed:	
Documents to be read alongside this policy:	Information Governance policies & procedures Community Pharmacy Contractual Agreement 2005 General Pharmaceutical Council, Standards of Conduct, Ethics and Performance NHS Wales Choose Pharmacy acceptable use statement
Purpose of Issue/Description of current changes: This procedure has been developed to provide assurance and to enable LHB managers to respond to and deal effectively with notifications that are raised from the National Intelligent Integrated Auditing Software Solution (NIIAS) relating to pharmacists accessing patient record systems via the Choose Pharmacy application within community pharmacies.	

This document has been prepared by Digital Health & Care Wales (DHCW) and approved by the DHCW NIIAS Management Board, All Wales Chief Pharmacists Group and Community Pharmacy Wales (CPW) Board for adoption by Welsh Health Boards and community pharmacy contractors. The content of this document must not be changed without agreement by the Digital Health & Care Wales NIIAS Management Board, All Wales Chief Pharmacists Group and CPW Board.

3. PROCESS SUMMARY

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. A requirement of access to these systems is that there is a robust monitoring procedure in place to provide assurance that records are accessed appropriately in line with information governance policy.

This assurance will be provided by use of the NIIAS software. The NIIAS tool provides a mechanism

for identifying potential information governance breaches, in particular breaches of the current data protection legislation (General Data Protection Regulations and Data Protection Act 2018)

NHS community pharmacy contractors in Wales are required to have an information governance policy in place, this includes a requirement to have in place a procedure for the management of information governance incidents, and this includes investigation of information governance breaches. The NIIAS tool will be used to identify potential breaches that will be referred to contractors for management in line with the pharmacy information governance policy and procedures.

This procedure outlines the agreed mechanism for the notification of potential breaches by the Health Board to community pharmacy contractors and how contractors communicate the outcome of their assessment and investigation (where needed) to the Health Board.

4. INTRODUCTON

The security of patient data within Health Boards and contracted care providers has been given a high profile in recent years and the Information Commissioner's Office (ICO) now has increased powers, including the power to penalise organisations up to €20 million or 4% of global turnover for serious breaches. However, the negative effect on the organisation's reputation would arguably cause greater damage than a monetary penalty.

To assist Health Boards in continuing to keep personal information secure and confidential, Digital Health and Care Wales (DHCW) has provided NHS Wales with Privacy Breach Detection software, called National Intelligent Integrated Auditing Software Solution (NIIAS).

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

Potential inappropriate behaviour includes system users looking up records of:

- Colleagues* (see note below)
- Family member* (see note below)
- Neighbours* (see note below)
- Own records (always inappropriate behaviour)
- Any record which the user has no valid work reason to be viewing

General advice to healthcare professionals from regulatory and professional bodies[1, 2, 3] advises that healthcare professionals should not routinely prescribe any medicine to anyone with whom they have a close personal or emotional relationship (this would include family members and potentially neighbours) other than in an exceptional circumstance.) Exceptional circumstances could include:*

[1] Good practice in prescribing and managing medicines and devices, General Medical Council 2013 (updated 5th April 2021) https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/prescribing-and-managing-medicines-and-devices

[2] Medicines, Ethics and Practice Guide, Royal Pharmaceutical Society July 2019 https://www.rpharms.com/LinkClick.aspx?fileticket=HKrEo4Xvgqo%3d&portalid=0

[3] In Practice: Guidance for Pharmacist Prescribers, GPhC November 2019 https://www.pharmacyregulation.org/sites/default/files/document/in-practice-guidance-for-pharmacist-prescribers-february-2020.pdf

- no other person with the legal right to prescribe is available to assess and prescribe without a delay which would put your, or the patient's, life or health at risk or cause unacceptable pain or distress, and
- The treatment is immediately necessary to:
    - save a life
    - avoid serious deterioration in health, or
    - alleviate otherwise uncontrollable pain or distress.

If a healthcare professional prescribes in these circumstances, they must

- make a clear record at the same time or as soon as possible afterwards. The record should include the relationship to the patient (where relevant) and the reason it was necessary to prescribe.
- Tell the patient's general practitioner what medicines you have prescribed and any other information necessary for continuing care, unless (in the case of prescribing EC for somebody close to you only) they decline consent to share information with the GP.

Whilst this guidance relates specifically to prescribing, it would be prudent to consider the principles when supplying medicines under NHS regulations within the enhanced services framework.

An employee's ability to access personal information does not automatically grant them the right to do so.

5. USE OF NIIAS WITHIN THE CHOOSE PHARMACY APPLICATION

The Choose Pharmacy application the DHCW IT platform that underpins delivery of a number of community pharmacy services. This IT platform provides the basis to develop and expand on a range of services that can be carried out in community pharmacies. The IT platform:

- Creates NHS patient record, which is transferable between NHS Wales community pharmacies.
- Links to the Welsh Demographic Service (WDS) - The master source of the NHS number for an individual. It provides demographic details for the patient as well as which GP, and which GP practice they are registered with. It also provides the facility to search for English residents via the link to the PDS Patient Demographic Service
- Links with the DHCW MTeD (Medicines Transcribing and e-Discharge) system which generates and electronic an electronic discharge advice letter (e-DAL).
- Links to Welsh GP Record (WGPR) enabling pharmacists to verify current prescribed medicines to improve patient safety.

Access to the Choose Pharmacy application is currently restricted to pharmacists who have completed mandatory training and have been provided by a Choose Pharmacy account by NHS Wales. However, in the event that other staff groups (for example registered pharmacy technicians) become authorized users of Choose Pharmacy, this procedure will apply to them also. Access to the patient record systems outlined above introduces the need to ensure a robust audit process is in place to monitor access to electronic patient record systems. The NIIAS tool is available to Health Boards to provide this function.

The introduction of NIIAS does not alter the terms and conditions of the arrangements with any contractor, nor should it change them for their staff or the disciplinary process which may arise from a breach. Community Pharmacy contractors have an information governance policy which must

include a procedure for the management of information governance incidents as part of the NHS Wales contractual framework. The NIIAS tool will identify potential information governance breaches that will be communicated by the Health Board to the contractor who will review the potential breach in line with the information policy and procedures.

All pharmacists (and other staff members) employed by an organisation contracted to the NHS are required to include maintenance of confidentiality as a condition of employment. It has always been a condition of employment, and of professional guidelines, that access to personal information is on a strict need-to-know basis. The General Pharmaceutical Council, Standards of Conduct, Ethics and Performance, requires registered professionals to protect patient confidentiality, and members of staff for whom they are responsible are also required to meet the same guidelines. NIIAS is an additional means by which we can assure our patients, staff, the Health Board and the Information Commissioner that the information held is handled correctly and in accordance with the law.

A contractor must ensure that pharmacists (and any subsequent authorised users of Choose Pharmacy) are fully aware that personal information should only be viewed if there is a clinical or administrative reason to do so.

This means that pharmacists (and any subsequent authorised users of Choose Pharmacy) should not be accessing records inappropriately. For example: looking at their own health record (even to confirm that a clinical system is working correctly or to check test results) or the records of family, work colleagues, friends/acquaintances and so on, unless it is a requirement of their job to do so and that the access and subsequent provision of the service is appropriate. Choose Pharmacy users must not use details of family, friends or colleagues for 'practice' or training on a new system – there is a test pharmacy account and test patients that can be used in these instances.

If an individual 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 General Data Protection Regulation 2016.

Guidance on this process can be obtained from [insert name of] Health Board, Information Governance Department.

6. PROCESS FOR MANAGING NOTIFICATIONS RECEIVED FROM NIIAS

[Insert name of Health Board NIIAS monitoring team [HB]] will be responsible for monitoring community pharmacy staff access to data within the Choose Pharmacy application via the NIIAS tool.

Where NIIAS identifies a potential 'inappropriate access' by a pharmacist (or other authorised user) accessing the Choose Pharmacy application, *[HB]* will contact the relevant Pharmacy superintendent/owner of the pharmacy where the notification originated. The Pharmacy superintendent/owner will be required to take one of two actions as outlined in the NIIAS Workflow Process for Pro-Active Monitoring of Choose Pharmacy: (Appendix 1).

The Health Board may undertake the initial assessment where it is considered the most appropriate course of action e.g. where the potential breach relates to the pharmacy owner/superintendent.

1. *Pharmacist accessing their own record on one occasion*

- Issue a warning email for staff members accessing their own record on the first occasion (Appendix 2 & 3)
- Where the access has been made by the pharmacy superintendent/pharmacy owner, the Health Board will send the warning email.

2. *Pharmacist accessing their own record on more than one occasion or potentially accessing another person's record inappropriately* [A]
   - Undertake an initial assessment using the Potential Access Breach – Initial Assessment Form (Appendix 4) to establish whether there is a legitimate clinical or administrative reason for the staff member to have accessed these records 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 Health Board with the name of the person who will undertake the initial assessment within 5 working days.
   - The initial assessment must be undertaken within 10 working days from a date agreed between the superintendent/owner and the Health Board (which would account for holidays/sickness and other circumstances which may delay the assessment).
   - The outcome of the initial assessment should be communicated to the Health Board via the Potential Access Breach – Initial Assessment Form.
     - Where the assessment is resolved or a false positive[B] is identified – the NIIAS notification will be updated and closed
     - 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 go the investigation.

Notes:

[A] *Managing Deceased patient notifications*

All modules other than DMR (e.g. CAS, EC, Flu, EMS, IPS)

The Choose Pharmacy application prevents users from accessing the records of patients who are flagged as deceased within the WDS/PDS patient searches.

Any notifications generated for these modules (e.g. CAS, EMS, Flu and EC), consultations will occur as a result of a potential data recording issue in another clinical system. These notifications should be closed without contacting pharmacy owners/superintendents and a support call should be raised for the attention of the DHCW NIIAS team via your Health Board Service-desk.

DMR

Deceased patient notifications generated within the DMR module should be processed under 2 above. Access to deceased patient records is permitted for up to 60 days following death to enable NHS providers to record any relevant information. This allows community pharmacists time to close any DMR records appropriately where a DMR has been started but not completed. Failure to close DMR records within 60 days of death will generate a NIIAS notification. To prevent this, community pharmacists should follow-up incomplete DMRs and close them within 60 days of the date the DMR was started.

[B] False Positive

A false positive is a situation where there has been a NIIAS notification, but there was a legitimate reason for accessing the patient record. For example, many members of staff live and work in the

same community, so a 'False Positives' could flag where a pharmacist has accessed a colleague or neighbours record in the course of providing an NHS service. Additional rules and conditions have been incorporated into the NIIAS application to minimise these false positives. Where identified, it is expected that line manager or other appropriate person will be able to discount most of these false positives when reported via the initial assessment process, with or without the involvement of the staff member named on the notification. Once a 'False Positive' has been identified and justification has been received by the *[HB]*, it will be closed, and no further action will be taken.

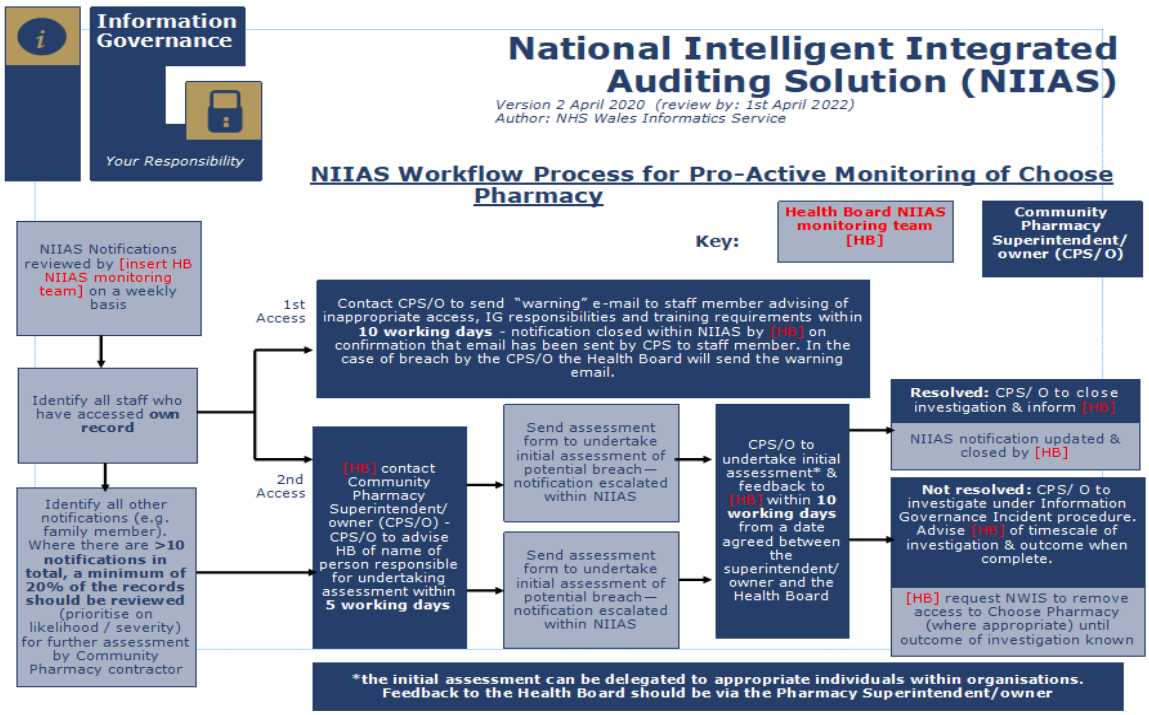
The introduction of NIIAS does not alter any of the policies of the Health Board or existing laws regarding access to patients' health records. NIIAS simply identifies and highlights instances where staff privileges are suspected of being abused.

Guidance has been developed to support contractors in managing potential access breaches identified by NIIAS (Appendix 5 & 6).

7. APPENDIX

APPENDIX 1

NIIAS workflow process for pro-active monitoring of Choose Pharmacy



APPENDIX 2

Notification Form – First Access of own record

National Intelligent Integrated Auditing Solution (NIIAS)

Notification Form - First access of Own Record

Assessment issued to:	Click here to enter text.
Date:	24/05/2016

During routine auditing, a potential breach of access has been notified for a staff member you currently line manage. You are required to send the staff member the NIIAS access warning email for this potential breach. Please ensure you fully read the "Initial Assessment Guidelines" before completing this form.

Please return the completed form to the [insert name of HB NIIAS monitoring team] at [insert name of HB] University Health Board within 5 working days.

Date(s) of breach:	24/09/2020
Details of staff member:	Click here to enter text.
Details of potential breach:	First access of own medical record
Action Required	Warning email to be sent
Date warning email sent	24/09/2020

Please return the completed form to [insert name of HB NIIAS monitoring team] [postal address] FAX: [insert] (Safehaven) email: [insert] within 10 working days.

Please mark all correspondence "Private & Confidential"

Departmental Use Only:

Required action taken: *Closed on NIIAS* ☐ *Closed on Register* ☐

APPENDIX 3

Notification of Access Breach

National Intelligent Integrated Auditing Solution (NIIAS)

NOTIFICATION OF ACCESS BREACH

You have received this e-mail as routine auditing using NIIAS has identified that you have breached your access rights by accessing your own patient record via the Choose Pharmacy application.

Your system access rights are provided to you to fulfil your role in caring for and providing services for patients.

You must not access your own record under any circumstances, and you must not access the following records (even with the individual's permission) unless you are directly involved in a professional capacity:

- Records of family or friends
- Records of neighbours or acquaintances
- Records of any individuals unless required to fulfil your role

Access to records you are not entitled to see is an abuse of your access rights and may lead to disciplinary action or even criminal proceedings under the Data Protection Act 1998 and the General Data Protection Regulation 2016.

You are entitled to request a copy of your own medical records under the General Data Protection Regulations and your request should be put in writing to the relevant medical records department. Alternatively, you may discuss your individual care, treatment or records directly with your care provider.

Any further instances of inappropriate access will result in your manager being informed and disciplinary action could be taken against you.

All staff are required to undertake appropriate Information Governance training and be aware of corporate Information Governance procedures. *If you are not currently up to date with your information governance responsibilities, you must contact your Caldicott Guardian within 2 weeks of receiving this e-mail.*

For further information about your information governance responsibilities please refer to your pharmacy information governance policy and associated procedures.

Insert [Pharmacy Superintendent details]

APPENDIX 4

Potential Access Breach – Initial Assessment Form

National Intelligent Integrated Auditing Solution (NIIAS)

Potential Access Breach – Initial Assessment Form

Assessment issued to:	Click here to enter text.
Date:	31/12/2015

During routine auditing, a potential breach of access has been notified for a pharmacist (or other authorised user) accessing the Choose Pharmacy application from the pharmacy premise detailed below. You are required to complete an initial assessment for this potential breach. Please ensure you fully read the "Potential Access Breach – Initial Assessment Guidelines for Community Pharmacy owners/superintendents & delegated staff" before completing this form.

Please return the completed form to the [insert name of HB NIIAS monitoring team] at [insert name of HB] University Health Board within 5 working days.

Date(s) of breach:	31/12/2015
Details of staff member:	Click here to enter text.
Pharmacy address	Click here to enter text.
Details of potential breach:	Click here to enter text.
Did the staff member require access to this information in order to fulfil their role?	Choose an item.
Was access found to be inappropriate / a breach of access?	Choose an item.
Please provide some detail about the identified reason for the notification:	
FINAL OUTCOME Referral made? *Only complete where further investigation has been undertaken*	Choose an item.

Please return the competed form to [insert name of HB NIIAS monitoring team] [postal address] FAX: [insert] (Safehaven), email [insert] within 10 working days.

Please mark all correspondence "Private & Confidential"

Departmental Use Only:

Appropriate access: *Closed on NIIAS* ☐ *Closed on Register* ☐

Inappropriate access: Choose Pharmacy access removed ☐ *Reportable to ICO* ☐ *Reportable to GPhC* ☐

Final outcome: *Closed on NIIAS* ☐ *Closed on Register* ☐

APPENDIX 5

Potential Access breach – initial assessment guide for community pharmacy owners/superintendents & delegated staff

National Intelligent Integrated Auditing Solution (NIIAS)

Potential Access Breach – Initial Assessment Guidance for Community Pharmacy owners/superintendents & delegated staff

What is NIIAS?

NIIAS is the abbreviation used for the National Intelligent Integrated Auditing Solution, which is a software tool available across Wales, used to detect potential misuse of access rights whereby pharmacists may have abused their access rights to view data they may not be entitled to view.

The purpose of the tool is to assist NHS organisations and service providers in complying with its Data Protection responsibilities and to give the public more confidence in the Health Board's and community pharmacy's ability to ensure confidentiality and privacy of personal data.

How does NIIAS work?

NIIAS uses intelligent data triangulation and audit logs to detect when a community pharmacist (or other authorised user) may have potentially misused their access rights within the Choose Pharmacy application. It then provides notifications to the *[insert HB]* Health Board *[insert name of team responsible for NIIAS monitoring]* for particular activity that may appear suspicious.

Examples of this type of activity are as follows:

- Whereby an employee accesses their own care record;
- Whereby an employee accesses the record of a family member;
- Whereby an employee accesses the record of a person living at the same address or a neighbour;
- Whereby a person accesses the record of a colleague.
- Employee accesses information about a person of media interest.
- Whereby a person has accessed the record of a deceased person

There will be instances where the above activity is perfectly acceptable e.g. a pharmacist may be responsible for the care of a neighbour; however, where a notification is generated an assessment of the event should be undertaken to ensure this is the case and that no breach has occurred.

Due to NIIAS being an All-Wales auditing tool, where a pharmacist has access rights extending across other NHS and partner organisations, this usage may also be included in any notifications received (e.g. locum pharmacists).

What should I do if a receive notification of a potential breach?

You will receive notification of a potential breach for assessment if potentially suspicious activity is detected within NIIAS for a pharmacist who has accessed the Choose Pharmacy application from a pharmacy premise you are responsible for. Where there are large numbers of notifications

generated, not all notifications highlighted within NIIAS will be transferred for assessment, as this would be an unrealistic expectation for the organisation to manage. The notification will be communicated via the Potential Access Breach – Initial Assessment Form

If you have received an assessment form for a potential breach, it should be treated in a confidential manner. The form will provide details of the pharmacist, date and details of the potential breach and further assessment fields for you to complete. The completed form should be returned to *[insert Health Board]* University Health Board *[insert name of team responsible for NIIAS monitoring]* within 10 working days of receipt:

Please return the completed form to [insert name of team responsible for NIIAS monitoring]
FAX: [insert] (Safehaven) within 10 working days.
Please mark all correspondence "Private & Confidential"

How should I manage a potential breach?

The process for the referral and assessment of potential breaches is outlined in the All Wales procedure for the auditing and escalation of pharmacists access to patient information systems via Choose Pharmacy, guidance has also been prepared to support the management of potential breaches - Guidance for the management of potential information governance breaches by NHS Wales community pharmacy contractors (Appendix 1).

When assessing a potential breach the following key principles should be considered:

- Did the employee require access to this information in order to fulfil their professional role?
- Was the information accessed in a professional capacity for the care, treatment or administration of an individual?

Where either of the above principles does not apply, it is likely that a breach has occurred and further investigation should be undertaken in line with the contractor Information Governance policy and procedure for managing information governance incidents. The need for further investigation should be communicated to the Health Board via the Potential Access Breach – Initial Assessment Form.

Serious breaches may need to be reported to the Information Commissioner's Office (ICO) who may see fit to undertake a criminal investigation. Where a serious breach is identified, it should be discussed with the company Information Governance Team to determine whether or not the breach is reportable to the ICO. Advice can be sought from *[insert name of HB]* UHB if required.

Where Fitness to Practice concerns are raised as part of the investigation of breaches, these should be managed in line with company procedures with referral to the General Pharmaceutical Council (GPhC).

Where can I find further information?

General advice and support on data protection issues, can be found on the Information Commissioner's Office website https://ico.org.uk/

Further information on the NHS Wales Information Governance requirements can be found via the DHCW website http://www.wales.nhs.uk/DHCW/news/25506

APPENDIX 6

Guidance for the management of potential information governance breaches by NHS Wales community pharmacy contractors

This document is intended to offer guidance on the assessment of potential access breaches in the event you receive a NIIAS notification related to one of your employed staff members or a locum employed to provide NHS pharmaceutical services via the Choose Pharmacy application.

Potential staff breach as identified by NIIAS	Potential (inappropriate) reasons for breach	Suggested management action
1. 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. Practising on a system using familiar names.	<u>First Access</u> If a pharmacist (or other authorised Choose Pharmacy user) accesses their own their own health information on a single occasion, within 10 working days the Pharmacy superintendent/owner of the contracted pharmacy where the breach occurred will be notified by *[HB]* via the First Access of Own Record Notification Form The Pharmacy superintendent/owner should issue a 'warning' email, sent directly to the individuals NHS E-mail/and company email account (if applicable). A hard copy can be sent to the staff member if required by the employing organisation. Pharmacy superintendent/owner to provide confirmation to *[HB]* of action taken via the First Access of Own Record Notification Form. The Health Board may issue the 'warning' email where it is considered the most appropriate course of action e.g. where the potential breach relates to the pharmacy owner/superintendent. <u>Second Access</u> If a pharmacist (or other authorised Choose Pharmacy user) accesses their own their own health information on a second occasion, the Pharmacy superintendent/owner of the contracted pharmacy where the breach occurred will be notified by *[HB]* via the <u>Potential Access Breach – Initial Assessment Form</u>

Potential staff breach as identified by NIIAS	Potential (inappropriate) reasons for breach	Suggested management action
Staff member accesses their own health records (continued)		The pharmacy superintendent/owner is required within 5 working days to delegate responsibility for initial assessment to the line manager or other appropriate person responsible for the individual or pharmacy, the *[HB]* must be notified of the name and contact details of this individual. The initial assessment must be undertaken within 10 working days from a date agreed between the superintendent/owner and the Health Board (which would account for holidays/sickness and other circumstances which may delay the assessment). The assessment should include a meeting the individual for an 'informal / initial discussion' and explain why this is a breach of the Subject Access Rights under the relevant Data Protection legislation and inform the staff member that any further breaches may be dealt with in line with the organisations Disciplinary Procedure The Potential Access Breach – Initial Assessment Form should be completed and stored in the staff member's personal file. A copy should be returned to *[HB].* The Health Board may undertake the initial assessment where it is considered the most appropriate course of action e.g. where the potential breach relates to the pharmacy owner/superintendent. *Actions for consideration* The pharmacist should: • read the relevant GPhC Standards of Conduct, Ethics and Performance, • read the employing organisations Confidentiality Code of Conduct & IM&T Security Procedures • be reminded of their responsibility when signing the Acceptable Use statement for access to the Choose Pharmacy" clinical systems. • undertake any mandatory IG Training or complete the WCPPE Choose Pharmacy IG eLearning module Confirmation of all identified actions should be retained in the personal file of the member of staff.

Potential staff breach as identified by NIIAS	Potential (inappropriate) reasons for breach	Suggested Management action
2. 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.	Following receipt of a NIIAS notification, the Pharmacy superintendent/owner of the contracted pharmacy where the breach occurred will be notified by *[HB]* via the Potential Access Breach – Initial Assessment Form. The pharmacy superintendent/owner is required within 5 working days to delegate responsibility for initial assessment to the line manager or other appropriate person responsible for the individual or pharmacy, the *[HB]* must be notified of the name and contact details of this individual. The initial assessment must be undertaken within 10 working days (from a date agreed between the superintendent/owner and the Health Board (which would account for holidays/sickness and other circumstances which may delay the assessment)) to determine whether the individual had a legitimate work reason for accessing the record i.e. clinical / administrative. If there is a legitimate reason for access, this should be reported back to *[HB]* by return of the completed Potential Access Breach – Initial Assessment Form, giving the work reason for accessing the record(s). The notification will then be closed, and no further action will be taken. The Health Board may undertake the initial assessment where it is considered the most appropriate course of action e.g. where the potential breach relates to the pharmacy owner/superintendent. Management of access breaches If the assessment shows that the access was potentially inappropriate, the investigating individual should return the completed Potential Access Breach – Initial Assessment Form to *[HB]* to inform them that the notification is to be escalated to an investigation. The investigation process will be the contractor process for dealing with Information Governance breaches, sits outside of this policy, and should be undertaken accordingly. . At this point the access to the "Choose Pharmacy" portal of the individual being investigated will be considered and if appropriate, suspended, pending the outcome of the investigation. The outcome of the investigation should be shared with the Health Board.

Staff member accesses someone else's health records e.g. Child or other family member, neighbour, colleague, celebrity etc. (continued)		Each case should be fully investigated and dealt with appropriately dependant on the individual circumstances. In all cases where a staff member has inappropriately accessed someone else's health records even if on only one occasion, this should be investigated in line with the relevant contractor policies. Further support will be provided by the *[HB]* team if required. *Actions for consideration* The member of staff should: • read the relevant GPhC Standards of Conduct, Ethics and Performance, • read the employing organisations Confidentiality Code of Conduct & IM&T Security Procedures • be reminded of their responsibility when signing the Acceptable Use statement for access to the Choose Pharmacy" clinical systems. undertake any mandatory IG Training or complete the WCPPE Choose Pharmacy IG eLearning module Confirmation of these actions should also be retained in the personal file of the member of staff *Referral* In the case of an inappropriate access to patient record being identified, the Pharmacy superintendent/owner should consider whether referral of the incident is, appropriate (e.g. GPhC/Information Commissioners Office). Referral should be communicated to the *[HB]* by updating the Potential Access Breach – Initial Assessment Form

Potential staff breach as identified by NIIAS	Potential (inappropriate) reasons for breach	Suggested Management action
3. Staff member shares information they can only know as a result of their employment or accesses someone else's personal information and shares the information 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.	In the event that a pharmacist (or other authorised Choose Pharmacy user) is suspected of sharing any information with a third party, the pharmacy superintendent/owner will be notified as described in (2) above. The Pharmacy superintendent/owner should undertake an initial assessment as detailed above. *Where the balance of probability indicates that patient information has been shared or disclosed to a third party, the contractor should consider whether this constitutes gross misconduct and manage in line with contractor HR policy.* The Health Board may undertake the initial assessment where it is considered the most appropriate course of action e.g. where the potential breach relates to the pharmacy owner/superintendent. *Referral* In the case of an inappropriate access to patient record being identified, the Pharmacy superintendent/owner should consider whether referral of the incident is appropriate (e.g. GPhC/Information Commissioners Office). Referral should be communicated to the *[HB]* by updating the Potential Access Breach – Initial Assessment Form