Template Standard Operating Procedure (SOP) for monitoring clinical access to the Summary Care Record (SCR)

<Put your logo here>

Policy Prepared By:	
Date Prepared:	
Policy Approved By:	
Date Approved:	
Review Date:	

Instructions for using this template:

Information in this template which is highlighted needs to have local pharmacy details completed.

Suggestions for the content of your SOP is made in light grey font and is to be amended according to your agreed local business process.

Please delete this table once your SOP is complete.

Information Governance (IG), Community Pharmacy and the SCR

Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information. Community pharmacies MUST comply with all requirements, and must also comply with the NHS Care Record Guarantee

SCR uses the following IG controls to ensure that the Care Record Guarantee rules are adhered to:

- Authentication and Role Based Access Control (RBAC), controlled by Registration Authorities (RA) and smartcard roles.
- Permission to View (PTV), controlled within the SCRa itself . This is where a user records that they have the patients permission to access their SCR.
- Legitimate Relationships (LR), which in the Community Pharmacy setting is controlled through the alert viewer system.

This SOP covers the review of any accesses; those made in the usual course of business in a pharmacy (LR - Clinician Self Claim LR), as well as those made “in an emergency” i.e. recorded as accessed without a patient’s express permission (PTV - Access Alert).

Accessing the Alert Viewer

Access to the alert viewer system (via the NHS Spine Portal using a smartcard) is needed so the pharmacy can identify which patients have had their SCR accessed, and who made the access. The pharmacy is then responsible for confirming that the person making the access had a legitimate relationship with the patient at that time.

The person able to access the alert viewer needs to have the Privacy Officer RBAC code (R0001) enabled on their smartcard. They are termed as the “Privacy Officer”, ie. the PO. They will review the following Alert Types:

- Create LR (Self Claimed)
- Access Alert

Information to help confirm the LR (Self Claim alert type)

There are a number of sources of information which the privacy officer can use to help validate there was an LR when the record was accessed. This could be one or more of the following, :

- A corresponding entry on a patient’s PMR of clinical activity at a similar time
- A signed consent form, or EPS nomination
- Staff logs
- Free-text reason entered by the user on SCR (which is shown on the alert viewer)
- SCR accessed within “normal” working hours

Accessing SCR “in an emergency” (Access alert type)

If a user accesses SCR without a patients express permission then they will select the “emergency access” option. The PO can see these accesses and use the same additional sources of information to assess whether this was appropriate, plus any additional corroborating information specifically relating to the reason. E.g. English not a first language

Summary of PO activities

The PO will:

- ✓ Access the SCR Alert Viewer in order to identify all accesses made at the pharmacy
- ✓ Establish if a legitimate relationship was in place, and that emergency accesses made were reasonable.
- ✓ Mark any accesses which need further investigation as such on the alert viewer
- ✓ Mark all accesses deemed appropriate as closed on the alert viewer
- ✓ Escalate any access deemed as inappropriate to the relevant excalation point for further investigation, ie. the Operations Manager/Pharmacy Superintendent/Pharmacy Owner/Information Governance Lead

Escalation

The PO will report any accesses which require further investigation to :
The operations manager/ Superintendent/Pharmacy Owner

Where a satisfactory outcome still cannot be reached, then further escalation of any potentially inappropriate access will be made to the Area Team to manage accordingly (in accordance with usual IG/performance policy)

Sample **Privacy Officer process**

The Privacy Officer (s) for this pharmacy is/are **********

The process they will follow for monitoring SCR accesses and legitimate relationships is as follows:

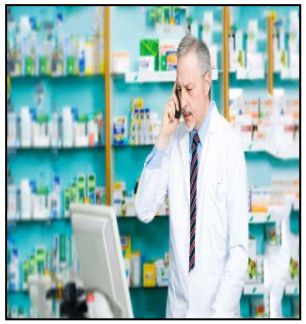
The table below lists a number of decisions and the subsequent approach your organisation could then take to detail your own local PO procedure. It is intended only as a guide to help you to determine your local preferences, timescales, frequency and sources of information to ultimately then complete your PO business process. You should select your own organisations response for each decision. Your decision chould be primarily based on usage and will need to be reviewed over time.

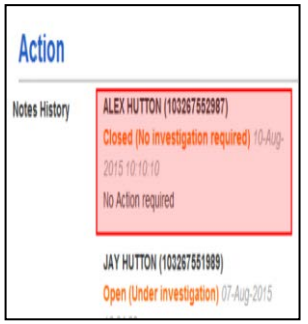
Decision needed:	Example A	Example B	Example C	Example D	Enter your choice here
1. How often will you carry out PO reviews?	Weekly	***Monthly***	Quarterly		
2. For organisations with a number of sites, determine the likely No. of pharmacies the PO is responsible for to be reviewed in each period? (N/A for a sole trader)	All	***50%***		5 sites	
3. When performing a review, for what time period of records that have been accessed will you check?	Every week	Random months	***Random weeks***	Random days	
4. How many access made in the defined review period will you check?	***All***	50%	Random sample of 3(?)/10	None	
5. What sources of information will you use to confirm the legitimate relationship?	Entry on PMR	Nomination for EPS OR Signed consent form	***Signed consent form OR Entry on PMR OR Free text on alert information***	Free text on alert information	
6. Will you complete any other random audits? EG. Check all of a random users accesses, or any access made between 6pm-8am?	6 monthly	Quarterly	***Monthly***	No, we wont perform this audit	

For example, if the examples highlighted in Bold and Italic were chosen, the business process would be as follows:

1. **Once a month** (decision 1) the privacy Officer will randomly identify and select **50%** (decision 2) of the sites within their organisation to review.
2. For the preceeding month, they will identify **1 specific weekly period** (decision 3) for which **all** (decision 4) accesses to SCR will be identified. *Essentially the PO is reviewing one quarter of alerts that have been made in the month.*
3. The PO will go onto the alert viewer system and may also produce an alert extract for the specified period, for all relevant pharmacies to show all accesses to have the access confirmed.
4. The PO will get the necessary evidence for matching from the phamracy, either as a ***report from the PMR or evidence of the consent form*** (decision 5). (This could be over the phone if responsible for more a number of branches).
5. The PO will match NHS numbers from the evidence against records to be checked from the alert viewer.
6. The PO will also select one user by random and check all accesses they made (decision 6).
7. Any records that have been accessed but associated evidence is not provided will be marked as under investigation. All other alerts for the overall monthly review period covered will be closed.
8. The PO will escalate these patient entries to the superintendent/lead pharmacist/IG Lead for onward investigation and action accordingly (as per any breach of Information Governance).
9. The superintendent/lead pharmacist/IG lead will inform the PO of the outcome of the investigation in order to close the alert accordingly.

Business Process – Alert Checking





Privacy officer due to review alerts	Access Alert Viewer	Review alerts	Confirm details with pharmacies	Close alerts
Weekly	self claim LR	missing info	verify reason	open - new
Monthly	access alert	time access	opening hrs	open – inv.
Quarterly		pharmacist	pharm. log	
		patient	PMR info	no inv. req.
Smartcard				inv. no action
N3 link		PMR access	make notes	inv. act. taken
			esc. issues	
Location				log