Community Pharmacy Summary Care Record (SCR)

Privacy Officer End-user
This Privacy Officer module:

• Is designed for all staff with the responsibility of monitoring alerts and auditing viewing activity in community pharmacy

• Summarises how to monitor alerts and audit viewing activity

• Suggests some best practice to help
Consent and Patient Choice Recap

Creation of an SCR:

• Patient can opt out or in at any time as often as they like

Viewing SCRs:

• The patient asked permission to view before health professional can access their SCR

• Emergency Access is available to some users if permission cannot be obtained e.g. the patient is unconscious or confused

• Alerts can be generated when SCR is used

• A Privacy Officer needs to monitor these alerts
Privacy Officer Role and Responsibilities

The Privacy Officer role can be:

• Specifically for the purpose of SCR; or
• Incorporated into the existing IG function of an organisation

The Privacy Officer should:

• Receive alert notifications
• Investigate alerts e.g. matching a self claimed LR alert to the local record of patient care (PMR) or identifying unusual patterns of Accesses
• Escalate inappropriate accesses
• Ensure local IG processes incorporate SCR viewing activity e.g. Information Governance Policy, Confidentiality Policy
Alert Generation

• Alerts will be generated when a pharmacy staff member views an SCR and that action needs to be verified and/or investigated.

• Alerts will identify the patient whose record has been viewed, the user that has viewed the record and the site the access occurred.

• The following actions will generate an alert:
  ▪ Use of clinician self claimed LR
  ▪ Use of Emergency Access
Monitoring Alerts

- When an alert is generated, a notification will be created and sent to the person responsible for monitoring the alerts.
- These notifications can be switched off and reports should be run instead on a regular basis for monitoring and investigation.
- The tool for monitoring and managing alerts is called the Alert Viewer.
- Each organisation must ensure that they have a nominated responsible officer (normally the Privacy Officer), with the correct RBAC on their smartcard, to access this tool and manage the alert process.
Alert Notification Text

Subject: Alert Notification

urn:nhs:names:services:lrs: Create LR (Self Claimed) alert on 19-Jun-2014 12:33:20 by This will be the site code

Alert Id: 7E07F1A7-A924-4FF1-B8A9-D44FFA4FCB72

This message is sent automatically based on information held on the Spine. To stop receiving alerts, please contact your local Spine administrator. Please do not reply to this email.
Email Notification in Alert Viewer

Email alerts can only be received by emails with the following extensions:
@nhs.net/uk - @gov.uk - @mod.uk @police.uk - @Cjsm.net
Alert Types

- All of the alert types will need to be managed but some are more common than others
- How they will be managed will be decided by the local organisations IG policies and procedures
Locum Accesses

- Regular locums should have the sites ODS code assigned to their smartcard.
- Irregular Locums will have a generic code on their smartcard (FFFFF).
- Whatever type of access they perform, they (irregulars) should record the site ODS code into the comments box.
- This can then be cross-checked with that day’s staff logs.
Comments Box

NHS Summary Care Record Access Management

STOP. Has this patient given permission to view their Summary Care Record?

- **Yes**
  - View record

- **No**
  - Access refused

The usual legal ethical and professional obligations apply when accessing a patient's clinical record.

- **Emergency Access**

Do you need to access the record for other reasons?

- **Other access options**

Provide more information about the access (Optional)
Some privacy officers will be responsible for multiple sites

Within the alert viewer there is a facility to search for different ODS codes that are allocated to that Privacy Officer
Investigating Alerts

- IG alerts can be viewed using the Alert Viewer which enables:
  - The recording and storage of IG alerts with the capability to search, view and close alerts
  - The generation of IG alert notifications
- Alert Viewer is accessed using the Spine Portal or directly from the desktop
- Access is granted as part of the Privacy Officer RBAC role
Reconciling accesses

- Organisations are responsible for auditing accesses to their records and for providing responses to queries from patients requesting details of who has accessed their record.

- Required by Care Record Guarantee.
Example Business Processes for POs

- Business processes are needed for the Privacy Officer to define how to investigate alerts
- The following activities need to be included in these processes:
  - Receiving notifications or running reports
  - Investigating alerts e.g. matching a self claimed LR alert to the local record or identifying unusual patterns of accesses
  - Escalating inappropriate accesses to relevant parties
  - Closing and updating the alert status
Example Business Process

For Example:
1. reason for access
2. User error/training
3. Clarify Legitimate Relationship to patient
4. Corresponding entry in additional system(s)

Privacy Officer receives alert notification by email or runs extract report from the Alert Viewer

Access Alert Viewer, obtain alert detail, mark as “Open - Under Investigation”

For Example:
1. Emergency Access box contains sufficient information when combined with,
2. Patient attendance can be confirmed on local system and,
3. User was on site in the department when the access happened

Contact the user and ask for more details

Add details to the alert using the Alert Viewer

Was the access appropriate?

Yes

Update alert notes with relevant information and close the alert

End process Alert Closed

No

Follow local escalation policies on “inappropriate accesses”

For Example:
1. Contact Line manager
2. Contact user
3. Contact HR
4. Contact Patient
5. Contact Caldicott Guardian

Enough information to reconcile Alert?

Yes

No
Alert Tools Demonstration

- Demonstrations are available for the following:
  - Search, Update & Close
  - Subject Access Request
  - SCR Access Report
Auditing SCR Activities

- NHS organisations are responsible for auditing accesses to their records and for providing responses to queries from patients requesting details of who has accessed their record.
- Required by Care Record Guarantee.
- In order to run audit reports for SCR viewing activity, Privacy Officers can use:
  - The Spine Reporting Service (SRS) if the viewing system was SCRa (accessed via the Spine Portal).
  - Reports on the host system if the viewing system was an integrated solution e.g. Adastra or Ascribe Symphony.
A subject access request (SAR) as defined by the Data Protection Act 1988, is when a patient wishes to know who has looked at their information in that organisation.

- Not many patients make a SAR. Very Rare.
- Normally these are received via the organisations Caldicott Guardian or IG manager
- In the event that the PO can see multiple sites information should only be provided on the organisation/sites that the PO is responsible for
Audit Reports - Other types

When the viewing system is SCRa, various reports are available including:

• Users that have accessed a specific record
• Records accessed by a specific user
• Transaction detail report
• SCR Access Report

Access is granted as part of the Privacy Officer RBAC role
Privacy Officer RBAC Role

Privacy Officer

• S8002 : G8003 : R0001
• Admin and Clerical : Admin and Clerical : Privacy Officer

Activities :

• B0016 - Receive Self Claimed LR Alerts
• B0015 - Receive Legal Override and Emergency View Alerts
• B0018 – Receive Seal alerts
Additional Information

• SCR IG Pages
  
  HTTP://SYSTEMS.HSCIC.GOV.UK/SCR/IMPLEMENT/IG

• Alert Viewer user guide

  HTTP://SYSTEMS.HSCIC.GOV.UK/SCR/LIBRARY/IGUSEGUID.PDF

• Authentication and Role Based Access Control

  HTTP://SYSTEMS.HSCIC.GOV.UK/RASMARTCARDS/STRATEGY/RAOVERVIEW
Connect with us

Web: www.hscic.gov.uk/scr/pharmacy
Prezi: User Demo
Email: scrpharmacy@hscic.gov.uk
Twitter: @NHSSCR

Sign up to the SCR bulletin: http://systems.hscic.gov.uk/scr/signup