PharmacyVoice
Speaking up for community pharmacy

Briefing
January 2016

Governance of Shared Care Records

The role of the Privacy Officer

Background

Shared Care Records (ShCR), and in particular Summary Care Records (SCR), have been available for some years in secondary care and in certain areas within the primary care sector. The Summary Care Record is an extract of key information from an individual's GP record, including all known allergies and adverse reactions recorded for that patient on the GP system; all acute medications in the last 6 or 12 months; current repeat medications and discontinued repeat medication (if the GP system adds this data). Additional information, such as blood test results or blood pressure readings, can be added with explicit agreement between the patient and the GP practice.

After a pilot in community pharmacy in 2014/15, it was confirmed that the ability to access individuals' SCR should be extended to community pharmacy teams and that a national roll-out would take place across the community pharmacy estate from October 2015 onwards. The roll-out programme being managed by NHS England is taking place on a regional basis, but organisations wishing to roll out SCR across their own estate can do so at their own pace.

Once SCR access has been implemented within a pharmacy organisation, pharmacy team members (as for all other healthcare professionals) must only access the SCR for a patient when they have a legitimate relationship with them (i.e. when they are actually involved in the person's care at that point in time) and when they have the individual's permission.

Every organisation that has access to SCR must have a nominated role-holder who is responsible for monitoring the SCR viewing activity of their users. The role title of this person(s) is Privacy Officer. The purpose of this role is to manage alerts and to audit SCR viewing activity. Alerts are generated by end users when they claim to have a legitimate relationship with the patient and view their SCR, and if they claim to have needed a legitimate emergency access to a patient's record. The alert notifications are prompts to the Privacy Officer to investigate SCR access and to confirm justifiable use or to identify inappropriate access.

Both SCR and other forms of ShCR require robust governance arrangements and Pharmacy Voice advocates that there should be one process that is applicable to both. This briefing therefore refers to all forms of ShCR, including but not restricted to SCR.

Position Statement

Pharmacy Voice fully supports the principle of having a Privacy Officer, or a similar role, to manage the quality assurance process in community pharmacies with regard to access to Shared Care Records.

All community pharmacy organisations are already governed by arrangements (as listed below) that ensure patient confidentiality and requires declarations of compliance annually (and at other times if required).

- Information Governance Framework
- GPhC Standards for Registered Pharmacies
- GPhC Standards of Conduct, Ethics and Performance
- The Community Pharmacy Contractual Framework

Therefore, ShCR access should be considered in the same way as access to any other patient confidential data, taking into account these requirements.

There is a specific requirement to check SCR access alerts but it is good practice to do this for all ShCR accesses.

Privacy Officer Role

The number of individuals recruited to, or undertaking the role of, the Privacy Officer within different community pharmacy organisations will vary, depending on the number of ShCR access points and the degree of usage of the ShCR on a daily basis within the particular company. The Privacy Officer should be responsible for ensuring that an appropriate quality assurance process is in place.

ShCR Quality Assurance (QA)

Appropriate QA activity could include the following:

- Appropriate training is provided for all ShCR users
- Standard operating procedures relating to ShCR access are available
- Checks on alerts are carried out in a timely manner
- Anomalies identified during the checking process are followed up
- For single-pharmacist/owner-operated models consider
    1. Appointing another registered pharmacy professional within the team (e.g. pharmacy technician or a regular second pharmacist) as your privacy officer
    2. Where this is not possible, appointing another member of staff within the team as your privacy officer
    3. recording access to the SCR on the PMR where the person accessing the ShCR and the PO is the same individual

Options 1 or 2 are preferred and recommended as they ensure “role separation” between the person accessing SCR and the person confirming it was appropriate.

Checking Alerts

There is no specific guidance on the number of alerts or the frequency of checking such alerts. Initially, checking in the range of 5-10% of alerts in a month might be appropriate, although this will depend on the individual circumstances of the business and the total number of SCRs the business is accessing. For example, one business may decide to take a few minutes each week to carry out the checks, whereas another may allocate more time to it on a quarterly basis. This range and frequency may be reviewed as processes become embedded into practice, or in the event of evidence of inappropriate access activity.

There is currently no mandate as to which individual alerts should be checked or investigated but there is a requirement for the PO to review the pattern of alerts at regular intervals to spot anomalies. Some examples of the circumstances in which investigation may be necessary are listed below:

- No record of the reason for access (where this is possible) is stated on the SCR
- Access is made to such records when the pharmacy is closed
- A higher number of accesses to records is being made by an individual when compared to other colleagues in the same company
- Repeated access to records is being made for the same patient
- There is a disproportionately high number of emergency accesses being made
- Unusual patterns of use are identified when reviewing trends

Disclaimer

This briefing is intended for information and guidance purposes only.