

Date: 1 May 2009

Paper for Information Commissioner's Office - Summary Care Records retention and deletion

Following our meeting on 2 April, the objective of this paper is to address the concerns that were raised and to explain our proposals for ensuring that the implementation of the Summary Care Record (SCR) meets all the requirements of Data Protection legislation.

CONTEXT

The SCR Programme is currently introducing the capability to create a Summary Care Record for patients in England. This was introduced to a number of Early Adopter Primary Care Trusts during 2007 and is now being rolled out to other Primary Care Trusts in England.

Currently the **ONLY** content within the Summary Care Record is a GP Summary obtained from the patient's GP Practice. There are plans to extend the capability to create content for the Summary Care Record such as A&E department discharge summaries, however given current plans, the only content in the SCR throughout 2009 will be a GP Summary.

The controls in place to ensure that the creation of SCR is in line with the patient's preference currently rest within the local GP system. If a patient prefers not to have a SCR, this preference is recorded in the GP system locally.

In **future** this patient SCR consent preference will reside on the National Spine. A migration of patients' locally held SCR consent is required from all local GP systems to the National Spine. A programme of work is currently underway within the SCR Programme to undertake this migration. We would welcome further discussion on the migration options.

Once the migration is complete, the patient's SCR consent preference will be known nationally. This will prevent SCR content being added where a patient has dissented from having a SCR. This migration **must** take place before any non-GP content can be added to the SCR.

CURRENT CONSENT OPTIONS

As part of implementing the Summary Care Record, patients are consulted through a Public Information Programme (PIP) on plans to create a SCR for them. If a patient wishes to opt out of having a SCR (Dissent), they are requested to inform their GP Practice prior to the record being created.

A patient can be in one of three positions:

1. They have not expressed a preference about their Summary Care Record.
2. They have explicitly consented to having a Summary Care Record
3. They have explicitly dissented from having a Summary Care Record.

Patient Takes No Action

For a patient who has not expressed a preference, their Summary Care Record will be created and maintained automatically. Users are able to access the record as normal under the Information Governance controls (see Appendix A).

Patient Explicitly Consents

For a patient who has explicitly consented, the creation of, and access to their summary care record is the same as for those who have taken no action.

Patient Dissents

Dissent is where a patient has explicitly stated they do not want a SCR. A patient can "Dissent" from having a SCR at any time. They can currently undertake this option by notifying their GP Practice.

For patients who have explicitly opted not to have a Summary Care Record, the situation differs depending on whether their choice is recorded by their GP Practice before or after their Summary Care Record creation.

Dissent prior to SCR Creation

If a patient responds with a preference to dissent prior to a record being created (currently 12 weeks), a 'blank' summary is created for this patient. No clinical information will exist for this patient on the Summary Care Record.

Subsequent Consent

When a patient who has dissented prior to a record being created subsequently changes their mind, they must inform their GP Practice of this. The GP Practice will record the decision, and will manually send the first clinical information, thus creating a Summary Care Record. The SCR will then be automatically updated under the normal Information Governance controls.

Dissent Post SCR Creation

If the patient has not dissented prior to a record being created and subsequently chooses to dissent from having a Summary Care Record, the data in the SCR is **logically deleted**. This means that pre-existing information is made invisible to all users and no more clinical information is added to the SCR.

Logical Deletion Process:

1. The patient must inform their GP Practice of their decision.
2. The GP Practice staff must record the patient's consent preference not to have a Summary Care Record.
3. A 'blank' GP Summary (containing no clinical content) is sent to the patient's SCR. This 'blank' summary replaces the previous summary. The previous summary is unavailable to users.

Once a record has been logically deleted, no data can be viewed, added or changed by system users.

These logically deleted records are only accessible to a small number of technical database staff employed by the database supplier and only when authorised by senior NHS CFH staff - a non-trivial and costly process. Although it would be possible to provide CFH back-office staff with the functionality to access these records (and the tool to provide this has been built), no CFH staff currently have access. We would need to consider allowing them access if the volume of activity became significant.

There are circumstances where there is a need to access pre-existing SCR information in a logically deleted record. The reasons for this are:

1. When the patient submits a Subject Access Request. (Response will be in accordance with Department of Health Administrative Guidelines.)
2. Where access can be justified for medico-legal purposes e.g. if evidence that Summary Care Record information existed which was relevant to litigation, complaint or an investigation.
3. To satisfy a Court Order that requires access.

These requests will be fulfilled in conjunction with the database supplier in providing access to the otherwise unavailable data using database tools only available to the National Application Service Provider database administrators.

In **future** and prior to the Summary Care Record being augmented by information from other care settings, these requests will be fulfilled by a small number of NHS staff with appropriate access. No one in the NHS currently has this level of access.

Subsequent Consent

When a patient who has dissented after the creation of their Summary Care Record subsequently changes their mind, they must inform their GP Practice. The GP Practice will record the decision and manually send up-to-date clinical information to the Summary Care Record. The information initially included in the Summary Care Record continues to be unavailable, and logically deleted.

PHYSICAL DELETION OF DATA

At our meeting we explained that it is Department of Health policy that health records that have been, or could potentially have been, used to support decisions about care and treatment should only be deleted in the most exceptional circumstances. This policy is strongly supported by the clinical professions, the bodies that regulate clinicians, those that indemnify clinicians against litigation and our statutory advisory group, the National Information Governance Board. As was explained at the meeting, this is why NHS record systems are designed without simple deletion facilities.

You indicated that you accepted that guidelines on the retention of health records were a health responsibility but were concerned that a small number of records may have been created where an individual did not choose to prevent an SCR from being created, or was not aware it was being created, and subsequently requests not to have one, with the understanding that the existing record will be deleted. Whilst we are not aware of any such individuals to date, we are prepared to authorise the **physical deletion** of these records where someone from the early adopted sites requests this, and where it can be established that care has not been provided since

the creation of the SCR in circumstances where the SCR could or should have been accessed.

We are not currently proposing to extend the option for deletion to anyone outside those who might have been misled, for the above reasons. The option will however be available where it is accepted that data should be deleted for persons who claim substantial harm or distress in line with the requirements of Section 10 of the Data Protection Act.

The following process is proposed:

Physical Delete Process

Where the physical deletion of a SCR is being considered, whether due to a patient being misled or in response to a section 10 notification, it will be necessary to coordinate action at a number of different levels. This will involve GP Practice staff, PCT staff and the NHS CFH SCR programme staff working together to manage the deletion process.

1. GP Practice staff must ensure the consent preference for such a record is set to "I don't want a SCR" on their GP Clinical System. This will logically delete the SCR and stop the previous SCR data being available to SCR users.
2. The extent that an SCR has been used to support care will need to be determined by analysis of audit information and this will be largely undertaken at PCT level with support from the SCR programme.
3. Where it is established that the record has not been used to support care, the SCR Programme will raise a service request for the National Application Service Provider to physically delete the patient's SCR record.

Enabling the differentiation of records that have been used from those that have not is not a simple IT check that a computer can do. (Some of the challenges inherent in this judgement are outlined in Appendix A.) It is expected that physical deletion will only be recommended for records that have not been consulted.

Physically deleted clinical data is permanently unavailable to all users, as it will no longer be present on the SCR database. The process will only be undertaken by forensically trained staff from the database supplier who can obtain access.

Once SCR data has been physically deleted, it cannot be made active again if the patient decides they want a SCR at a later time; a new SCR will have to be created.

PUBLIC INFORMATION MATERIALS

We confirmed when we met that we accept that publicity materials supporting the implementation of the SCR have emphasised that people do not need to have one if they do not want one and that they can change their minds at any time. We also accepted that some locally adopted materials have gone further and stated explicitly that when a patient changes his mind an existing, but now unwanted, SCR will be deleted. As you are aware, as soon as we discovered this, we asked the NHS body concerned to amend their materials and this was done.

As outlined in our letter, we have taken action to amend all public information materials and we would welcome your comments on the following draft wording for the public:

Patients can change their mind at any time. If they later decide to opt out of having an SCR, access to the record will be blocked and their record will not be available for clinical care or any other routine NHS activity. The record will not be deleted as it may be required as evidence when investigating the performance of a clinician or there is a dispute about the facts in a particular case.

As stated, we are prepared to authorise the physical deletion of these records where someone from the early adopted sites requests this and where it can be established that care has not been provided since the creation of the SCR.

APPENDIX A

SUMMARY RECORD CONTROLS

System Compliance

Only systems that comply with the SCR compliance requirements are able to connect to the Spine and gain access to send information to, or retrieve information from, the Summary Care Record. The Spine will only accept interactions from systems that are registered in the Spine Directory Service as Accredited Systems. Prior to this registration, the compliance process ensures compliance with the Information Governance controls including: Authentication, Role Based Access Control (RBAC), Audit, Legitimate Relationships (LR), Consent, and IG Alerts¹. These controls are described below.

Authentication

User authentication requires the user to be registered by a Registration Authority using eGIF level 3 standards, and to authenticate to the system by using their smartcard together with a Personal Identification Number (PIN). Thus all users of Spine systems must have been granted access by the Registration Authority.

Role Based Access Control

The user registration process associates the user with one or more roles. If the user has more than one role, then, at authentication time, they must select the role that they are currently operating in.

A particular role is associated with activities (mapped to Business Functions), allowing the user to perform some tasks. Without the associations, users are denied access to those business functions. In the context of the Summary Care Record, the main activities allow the user to:

- update the SCR
- retrieve information from the SCR
- create a Legitimate Relationship (see below), or
- change the SCR Consent Preference.

It is the responsibility of the Registration Authority to ensure that the activities available to each user are appropriate to their working position.

The RBAC control is enforced at run time by the local system.

Audit

Audit records are kept for each significant event by each system that participates in an update or retrieval process. For user initiated actions, the identifier of the user, and the identifier for their selected role, is recorded for each event.

These audit log records, taken together with the information content held within the databases, can provide a full record of which authenticated users gained access to,

¹ Other controls for Sensitive records and Sealed Envelopes are not described here. Security controls are not covered by this paper.

or updated, the Summary Care Record, and which information was requested to be viewed.

In the absence of the information within the databases, i.e. if the information has been physically deleted, the audit trail would reveal that the SCR had been updated or viewed, but not what it had been updated with, or what had been viewed.

If only the Spine audit logs are used for reporting purposes, this can reveal that information has been retrieved from the SCR, but not whether the user had viewed that information. The information might have been pre-fetched by the system to facilitate a fast response, but not actually requested by the user.

In the case of SCR Consent Preference changes, the history of the changes to preferences recorded over time is held within the Audit log records rather than the Access Control Service.

Legitimate Relationships

All access to the Summary Care Record by users of local systems is governed by Legitimate Relationships (LRs). The relationship is between the patient, as identified by their NHS Number, and a group of users or an individual user. The user therefore may have an LR with the patient either directly, or by virtue of being a member of the group of users.

LRs with the patient are normally created as part of a registration or referral process. In some circumstances, a user may need to gain access when an LR has not been created by the system and the user may grant access to a colleague, or the user may claim a relationship for herself or himself (a Self Claimed LR).

Because the creation of a Self-Claimed LR can be carried out by an individual acting alone, a privacy officer is made aware of this event by the generation of an Alert.

Consent - The Summary Care Record Consent Preference

Local Opt-out Flag

When a patient chooses not to have a Summary Care Record, at present the record of the decision is only held in a GP system, and the control is enforced by the GP system software. The control operates in three logical places:

1. If no record yet exists, a blank GP Summary is created and therefore no clinical information exists in the Summary Care Record. (The blank Summary contains text explaining the patient's choice.)
2. If a GP Summary already exists, then a new 'blank' GP Summary replaces the existing GP Summary. (The blank summary contains text explaining the patient's choice.)
3. Other GP Summaries (ones that are replaced or potentially withdrawn) are not available to users. For existing GP Systems (those using the older query interfaces), this protection is under local system control.

Central Opt-out Consent Preference

The use of local flags, (flags available only within a single GP system) is being replaced by the use of centrally held preference information in order to be available to all Spine-connected systems. The control will operate once the migration of local flags to the central Access Control Service has taken place. The central elements are in place now.

