PHCSG CLICSIG report on Shared Care Records v1.1

Meeting July 2020

Contents

1 Foreword

This report is the result of an exploration of risks and concerns about the use of shared patient records carried out by Clinical Special Interest Group (CLICSIG) of the British Computer Society's Primary Health Care Specialist Group (PHCSG). The topic was the subject of several meetings, starting in 2008, and culminated in two virtual meetings held in June 2020. As the use of, and interest in shared records is spreading, understandably because of their potential to ensure more coherent - and so better – patient care, the PHCSG considered it timely to publish their findings and the conclusions drawn from them.

1.1 The report is intended for reading by general practice clinicians, informaticians, standards developers, clinical system developers and others with an interest in making the union between information technology, informatics and medicine deeper and more fruitful. Although it originated in primary care, we believe it will be of use to clinicians, health informaticians, system developers and information policy makers generally.

1.2 Here is a glossary of acronyms used in the report. Acronyms are shown in bold wherever they appear in the document.

CSR	**Composite shared record – a** kind of **shared** (patient) **record** consisting of fragments of records of prime entry created by one or more organisations caring for the patient, where a contributor considers that others caring for the patient need to be made aware of the information the fragment contains.
DOI .	**Digital Object Identifier –** a string of numbers, letters and symbols used to permanently identify an article or document available on the web.
LHCR	**Locality Health Care Record** – a patient record that provides summary information about the care provided by organisations within a locality, typically a region that can be considered to offer the full range of health facilities. Whether a LHCR should include information about residents in its area from units providing specialist services nationwide, such as Papworth, Broadmoor, Stoke Manderville., etc is currently an open question. Many LHCRs are taking the form of a Composite Shared Record.
PHCSG	**Primary Health Care Specialist Group**- a specialist subgroup of the British Computer Society.
PRSB	**Professional Record Standards Body** - the body which sets standards for healthcare records.
QOf	**Quality and Outcomes Framework** – one of the ways in which GP practices are remunerated (for hitting targets).
RBAC	**Role Based Access** Control - the use of a role type to control the kind of data that someone – e.g. a clinician - can see
SR	**Shared Record** (of any sort), usually where contributors share all or part of their own patient care records of prime entry about a patient

SNOMED	**SNOMED** is a commonly used abbreviation for SNOMED CT, which is the official term for the structured clinical vocabulary mandated for use in English health records. Its full title is the Systematised Nomenclature of Medicine - Clinical Terms.
SSEPR	**Single shared electronic patient record -** a synonym used currently to describe the SystmOne **SSR** (see below).
SSR	**Single shared record—** the preferred term in this report for a single record of prime entry used by two or more care organisations as their **sole** repository for patient information. Save as requested by the patient or required by the law, the entire record is visible to all the organisations using it.

2. Introduction

2.1 Types of Shared Patient record

We recognized two types of shared patient record currently in use or being developed:

(a) Single Shared Record (**SSR**) where *two or more organisations use the **same** patient record of prime entry.* The SystmOne Electronic Patient Record is the only example in use to date (March 2021).

(b) A Composite Shared Record (**CSR**), where *care organisations contribute fragments from their own patient records of prime entry to a single multi-organisational read-only record for use by other care organization treating their patients, e.g. their general practices*. Many of the Local Health Care Records (LHCRs) being constructed at regional level take this form. A (significant) number of these are referenced in the Final (reference) report of the Shared Record Professional Guidance [1] written by the RCGP in 2011

2.2 The approach taken

We decided to take a clinical safety approach to capturing our concerns. So a modified Hazard Log was created during the discussions and then shared and developed further. The assessment of a risk level was deliberately left out as that was not felt to be part of this exercise. The log was not intended to be exhaustive, but to highlight areas of concern for further discussion and mitigation.

The next section of the report (section 3) describes the issues we discovered, and section 4 the clinical concerns that emerged from these issues.

3. Review of clinical concerns about Shared Care Records.

The following is a summary of areas where hazards were identified by the group. A fuller description of the hazards can be seen in the appendix and the hazard log.

3.1 Audit Trail.

Concerns were raised around maintaining an audit trail in a shared care record, especially if editing is allowed within that record, as we believe it must be to deal with erroneous and/or duplicate entries. More generally concerns were raised over the loss of audit trails with the demise or a change of host

---

1

Currently the SPRG is not available on the RCGP website.

systems, particularly where they had contributed to a shared care record. We recommend that a national solution is sought for this, and what follows outlines how this could be done.

The key step would be to log any change made to a record entry in the patient database as a change log entry in the patient record itself rather than in a separate audit file. Each change log entry would record the change being requested, when, by whom, why and any patient data added / removed / changed / assigned a different status. Placing a visible flag in the patient record would alert the user to the presence of a change log entry, which could, with the addition of the relevant facilities to the application software, be used to create a version of the patient record as it was at any time in the past. It would however require a viewer to be available for the record for as long as the database concerned exists.

Changes to the payload of a record entry should be made by the organization of prime entry and propagated to any organisation that has received a copy of it , e.g. as part a composite shared record.

This would **not** remove the normal requirement to back up the complete database at intervals to mitigate the (very different) risk of it being destroyed or becoming unusable for some other reason. Such backups would include any change log entries in the patient database.

3.1 Curation of Records.

EPRs are dynamic records and to enable good care need curation facilities to enable erroneous entries to be relegated to a change log entry in the audit trail. Curation is usually under-valued, currently very rarely performed and even more rarely budgeted for. Curation is more important than ever for shared records. Who curates a record and when and from what perspective is recognized as a hazard: the general rule is wherever possible data should be curated by the organization - and ideally the person - that generated it. However keeping the audit trail as part of the record as proposed above in 2.3 would enable curation considered inappropriate to be undone, and then done differently if required. This process could be repeated ad nauseam. It would be helpful to visibly show places in the record where curation has occurred, and which could be used to access the corresponding change log entry in the audit trail.

3.2 Data Quality

Poor data quality can significantly affect good care. The lack of proper training in the use of EPRs and data quality is felt to be a significant contributor to this hazard. The better design of systems and the use of templates can mitigate this risk to some extent.

3.3 De-duplication

Shared care records will encounter multiple entries for the same event. In some cases, it is easy to resolve as only one event such as a hysterectomy can ever take place. In others, e.g. myocardial Infarction, deciding whether it is one or multiple events is more difficult. Accurately recording the dates of each occurrence usually resolves the problem. Many Shared Care records integrating multiple records will use an automatic de-duplication process and we believe it should always be clear to the user that this has happened. If all data removed or changed, plus who made the change, why and when is retained in a change log audit trail material in the patient record itself as suggested in 2.3, this would make de-duplication visible and its resolution possible if required.

3.4 Erroneous/Disputed entries

In both single shared records and shared care records issues arise where a data item is felt to be either erroneous or disputed. Where it has been entered by a different organization, correcting it should be done by the originator, probably after prompting by the recipient. We recognized that one solution was to have an executive body to take responsibility for this and ensuring there are appropriate ways to manage it in a timely manner. It was also felt that there should be the ability to flag a data item as erroneous or disputed or simply a concern, so that it is treated with caution if it cannot be resolved. The audit trail mechanism suggested in 2.3 would record this change in status of a data item, as it would any change to the item itself.

3.5 Legal Issues

Concern was expressed about third party data and the risk that it may be inappropriately shared. The group noted that there is currently no way of flagging data (and therefore identifying) data as about and /or provided by a third party. We felt this must be explored, ultimately with a view to routinely identifying third party data at the time of recording, and where it is provided by the third party, asking if it may be shared it with others caring for the patient, and whether the patient should be made aware of it.

3.6 Role-based access controls

Role Based access was not felt to be granular enough to ensure that data is only seen by those who need to see it. One mitigation is to ensure regular audit of record access, so that inappropriate access was highly likely to be discovered. Under the COPI regulations this has been relaxed for direct care and it would seem to make sense to keep this relaxation making data sharing much easier across NHS/Social Care for the purposes of direct care.

3.7 Retention limits for Safeguarding & child protection conference data

Safeguarding data and information around child protection conferences may have retention dates after which the data must be removed. This becomes difficult to ensure where the data is shared and copies are created in other records. It is essential if this is permitted that the retention date is also shared and acted upon by the receiving system.

3.8 Problems with accessing legal documents.

Advanced directives, powers of attorney and other such documents may be referred to in the shared record but the original document are not available. The group supported the idea of a national repository for such documents, so they are accessible from all records where they are relevant.

3.9 Medication in both SSRs and LHCRs

The hazards around medication were focused on the

- inability of one organization to alter the medication prescribed by another in the light of changes to the patient's condition since it was originally prescribed and

clarity about who is responsible for on-going prescribing.

The concept of a single medication record for a patient, perhaps even a single national medication record, was felt to be an idea worth supporting but would not overcome the problem of who is responsible for the overall medication of the patient when care passes from one organization to another.

3.10 Creating a record structure for shared care records.

The way in which a record is structured and laid out is important in ensuring that significant data is not overlooked, and there are likely to be different conventions in primary, secondary and community care. Creating a shared care record is likely to require semantic interoperability between disparate record structures. There is a risk that context and provenance is lost in sharing where contributing records have different structures. There is a case for more similarity in the structure of EPRs where it can be had without degrading their content.

3.11 Creating referrals from shared records

When data is shared in a record - especially a single shared record - there is no clear guidance on how much information needs to be included in a referral and how much can be derived from the record visible to both parties. Good practice should be agreed across organisations sharing their records.

3.12 Responsibility for care

Where two or more organisations are caring for the same patient and a new hazard is identified and it may be unclear who should be responsible for acting on information newly recorded in it, e.g. when a test result comes back, and a consultant and GP are both involved in the patient's care. Solutions to this should be agreed by the professions, nationally adopted, and their use monitored. Consideration should also be given to mechanisms to embed formal requests for a hand-over of care in system design, allowing for acceptance or rejection of the request by the recipient.

3.13 Resolving conflicts between treatments managed or proposed by different clinicians for different problems.

This problem also occurs where shared records are not used but is likely to be noticed sooner and more reliably when they are. This requires a code of practice to be in place and used when significant change is proposed to the care plan for an existing problem / a care plan is proposed for a new problem.

3.14 Teaching and implementation

The group recommended on-going support and training in the optimal use of systems for patient care (and not just at the induction of new staff or at initial system deployment,; and better training throughout clinical education for all care disciplines in the use of EHRs, data entry and the importance of keeping high quality electronic records.

3.15 Terminology

There should be agreed and mandated standards for record-keeping across agreed care pathways, mitigating for differences in systems. Snomed terms should be used at a minimum for all non-numeric data used for algorithmic decision support. All staff using and /or entering data into patient records – not just doctors - should receive ongoing education and training in how to use and update patient records, including an appreciation of the different hierarchies available in Snomed.

3.16 Usability

Users should be involved in the design of systems. Poor usability can make the system difficult to use effectively. It needs to be recognized that users from different specialties and different organisations will need different views of the data. One size will not fit all.

3.17 Value sets

List of concepts are increasingly being used to constraint data entry in particular circumstances, in order to increase data quality. But unless they are kept up to date and are error-free, they will have the opposite effect.

3.18 Be aware of the possibility of systematic incompleteness in shared record content

The patient may be undergoing treatment at a care unit that is not submitting data to his or her Shared Single Record or Composite Shared Record, One example would be an episode of care at a national centre of excellence such as Great Ormond Street or a care unit outside the patient's locality. Arrangements must be made/ continued to ensure that the data generated by the associated episode of care is captured in the patient's GP record.

4 Conclusion

A hazard identification approach was used in this report. It was not intended to be comprehensive or to allocate levels of risk, but to draw attention to these hazards in order that they can be discussed more widely, and their inherent risks better mitigated.

The themes which come out in the hazards outlined above are as follows.

Education

Many of them rely on education and training of the users to mitigate the risk. Generally, there was felt to be lack of education – and of educational resources & best practice agreement on the use of EPRs and that this needed to be addressed at all levels of medical & other user education. It was also felt that where there was training in the use of clinical systems it was often only at the deployment of the software or induction of new users & restricted to use of the software, not its use to enhance patient care, and was not followed up on a regular basis to enable users to enhance their use of the tools.

Better and more thorough training would mitigate the issues around terminology, using the structure of records correctly and curation of the records to maintain high quality, as well as issues around the use of third-party data and appropriate access to and use of safeguarding information.

Software Design

The design of shared care records. Ensuring high levels of usability by involving users in the design and ensuring it supports the workflow will lead to better quality use of the systems. There are issues around specific data types and how they are managed, such as safeguarding data, and legal data, including subjects such as retention dates. Taking these into account in the design of Shared Care Records is vital, as is ensuring the context and provenance of the data is preserved to ensure that the data becomes usable information. Given the variance in data structure in contributing systems this is a challenge, but it is essential to make sure that the record can be viewed from a variety of aspects, such as a problem list or an encounter view and not just as a flat list under section headings. Where possible all the relationship links of a data item should be preserved, and the data viewed in the same structure as the contributing system.

De-duplication

For shared records to make sense de-duplication of data items needs to take place. But it was felt to be important that where this had occurred the fact was obvious and the discounted data items could be seen if required, to retain the integrity of the record.

In a socio-technical model these design issues are the "Informatics layer", the level where it is agreed how things will behave and how data is stored and accessed.

The "Conversational Layer" in this model is around agreeing the processes and how they will be used. Several of the hazards above can only be mitigated by ensuring this is undertaken. A solution to this would be for shared record systems to have an executive group who can gain agreement from users on how the system will be used. They should own the ultimate risk. This would enable issues around responsibility for care, hand overs of care, for prescribing, and record curation to be clarified, as well as issues where data was disputed or felt to be erroneous.

The top layer of the model is around socio-cultural matters. These are issues outside the systems themselves, such as the data governance laws. But it could also be seen as concerns that need to be dealt with once, subject to ongoing scrutiny and /or action by the professions. Getting education into the training curriculums, providing input into creating, monitoring, and maintaining the necessary standards and providing on-going training in keeping high quality EPRs cannot be addressed at system level only and need a national approach. Taking a high-level view of the data models needed in clinical systems to serve the new purpose of sharing data would also mitigate several of the hazards arising from the different data structures in/ of contributing care record systems.

Summing up

The PHCCSG recognizes the huge benefits to patient care of having comprehensive and up to date information about them and their care, and the roles of shared care records in achieving this.

This report highlights problems which we have been talking in creating and managing shared records and suggests proposals that the Group believe would mitigate them. The group has been discussing many of them since 2008.

We would like to see this report used as the basis for a safety case to justify the work needed to resolve them. However, some of the most serious hazards – for example the lack of education in record keeping, and agreement about clinical behaviour in certain situations - need urgent resolution at a professional level, to create norms for the use of all shared records.

Appendix

Description of identified hazards in shared records

Audit Trails

1. **Hazard Name: Lack of ability to reconstruct the database as it was at any time in the past.**

Risks: Failure to support the ability to recall the patient's or clinician's view of care at any specific time in the past, leading to psychological harm to patient or reputational damage to the clinician, which might have legal consequences for either.

Audit trails are an important part of any electronic patient record, (and in particular any temporarily jointly-assembled record) allowing the record to be reconstructed as it was at a particular point in time, often for medico-legal purposes. Shared records which construct a view of multiple sources of data on the fly present a particular challenge. One solution might be to keep an audit trail of the data published and consumed; what data was published and what viewed. The source systems' audit trails should be able to reconstruct what data would have been published (i.e. visible to the user) at that point in time.[2]

There was agreement that changes to the content of Shared Care Records should be made in the contributing source's system. Furthermore, with any shared care record, agreement should be sought at the outset on how data can be edited, and what was the appropriate way to edit it, so that the provenance of any change can be ensured and the reasons for change noted. Users need to be educated about this and guidance should be available.

A question was raised about the preservation of an audit trail when a system that has contributed to a shared record ceases to exist. The group recommended seeking a national solution for this. be sought.

Curating the Record

2. **Hazard Name: Information missed by failure to curate the record**

Risks: Important data may be missed out or de-emphasised, leading to patient harm.

Without curation, EPRs could become cluttered with minor or irrelevant items, historic items could be shown as current, and important data items could appear under the wrong headings or be de-emphasised because of their placement in the hierarchy. This becomes of more importance when the data is shared.

There should be a policy on record curation, and a recognition both of its importance and the time taken to undertake it. In relation to shared care records, the contributing organisations should be made aware of the importance of curation, and ensure that their staff are competent in curating the records. It was recommended that all data shared using a shared care record should be subject to agreed data standards.

2

Report of Newcastle CLICSIG 21st May 2016.

Record curation is a complex time-consuming exercise, and it was felt to be an area where AI might be deployed in future both to curate and present data relevant to each user.

3. **Hazard Name: Information loss by curation of the record**

Risks: Important data may be missed out or de-emphasised leading to patient harm.

There is also a risk that curating the record can lead to harm. This might occur if the curator has a different view of the importance of specific data items. This is of particular relevance where different disciplines are involved. What is important to a specialist may be radically different to a GP. Additional problems may arise if curation occurs in a different record structure, which changes the provenance of the item; or where there is uncertainty over who is responsible for a particular area of the record which is of common interest.

It was recommended that there is clarity in any shared care record about the importance of curating the records and who is responsible for what data items. It was also recommended that different organisations using a shared care record should be able to filter the data in a way which is suitable for their use, i.e., to create their own summary view of the data.

Data Quality

4. **Hazard Name: Poor Data Quality**

Risks: Data is not available when health care workers need it to make a diagnosis or adjust treatment accurately. Unnecessary repeats of investigations may be ordered which are unpleasant for the patient, inconvenient, create delays in diagnosis, waste resources, or block resources for others. Financial loss may occur in relation to outcome-related financial targets such as the Quality and outcomes Framework (QOF), leading to less investment in, or reward for, the health care organisation.

This can occur where:

- users are not confident in the correct use of terminology, leading to poor coding.

- important data is not coded but entered as free text.

- data from external sources are not captured onto the record.

- there is a lack of training in data quality and good practice in use of EPRs.

It was noted that QOF had led to better recording of those clinical areas reimbursed in Primary Care. It was also noted that in secondary care data was often entered specifically for remuneration purposes, and often not contemporaneously.

The importance of training and education in the use of terminology and EPRS at all levels of medical education and careers would help. This should be relevant to the needs and context of the users, and ready access to clear information and guidance should be available. Evidence of training in data quality should be an important part of any quality assessment of an organisation.

The use of data entry templates and the constraining of the use of the terminology by use of value sets in different areas of a record can contribute to better quality. Regular feedback on data quality in the form of targeted audit could also play a significant part in improving quality.

De-duplication

5. **Hazard Name: Data loss or corruption as a result of the de-duplication process.**

Risks: Clinician considers patient's condition more or less serious than it really is, and overtreats or undertreats the patient as a result.

The process of de-duplication of data, where it is supplied by multiple sources, may lead to the incorrect assumption that a patient has only had one event when in fact they had had multiple events; or that they had had multiple events when they had had only one. *It may not be clear from the record that a data entry has been de-duplicated and is therefore not visible.* These issues may occur where an algorithm is used to filter out multiple entries of what is considered to be the same entry.

It is recommended that where data has been de-duplicated the data item is flagged and that all data considered to relate to the same event should be accessible if required. It is also recommended that the process and potential consequences of de-duplication are clear to all users and included in training on the system.

Erroneous/ Disputed entries

6. **Hazard Name: Inability to correct certain data items.**

Risks: The true condition of the patient may be misunderstood, leading to patient harm

In a shared care record data items may be identified as being erroneous, not granular enough, or disputed. Where items were entered by another organization the current user may not have authority to edit them. The owner of the data may dispute its inaccuracy and there may be no method for resolving these disputes.

One solution in use is to have an executive organization, with representation from all contributing organisations, which would be the ultimate risk owner and would be responsible for commissioning the necessary software, training, end-to-end processes, and day-to-day running of the software and the service it supports.   Processes to agree these issues should be defined and users educated in their use.

It was also recommended that mechanisms should be available in systems to add an attribute or flag to an entry to declare it to be disputed or felt to be erroneous, together with a built-in mechanism to request author review.

7. **Hazard Name: Deletion of disputed or erroneous data**

Risks: Important data about the change, or what led to it, may be missed, leading to patient harm

Previous deletion of disputed or erroneous data means that the original entry is not visible to the user, other than in the audit trail. When data is deleted there should be an appropriate mechanism for easily and conveniently displaying the deleted data, the reason why it was removed, the date when it was removed and what was substituted for it.

This is mitigated in part by one organization currently not being able to delete data entered by another; and data should only be changed in the source system. Nevertheless, there should be mandated, professionally approved mechanisms in EHRs for deleting or editing entries; such corrective mechanisms should be facilitated by the system.

Legal issues

8. **Hazard Name: Third party data shared inappropriately.**

Risks: If the third party complains, the data controller may be fined by the Information Commissioner's Office (ICO) for breaching the General Data Protection Regulations (GDPR). In addition, the patient might sue the GP. The patient's relationship with the third party(ies) involved may suffer and thus damage non-professional care provision.

Patient safety may be put at risk if the identity/ whereabouts/ contact details of relatives of estranged/ abusive individuals is inadvertently revealed as a result of a data breach during, say, a download of a case file to a solicitor.

EPRs contain a variety of third-party data and there is no agreed mechanism for flagging this data. IT may be implicit in coding, contained in free text or an attached document. There is a risk of this being shared in a subject access request. The risk increases as the data is shared and more people and organisations have access to the data. This applies even more if shared records can be accessed via patient portals.

The group recommended that there should be an agreed universal mechanism to flag data as "Third-party", which would allow it to be automatically redacted in certain views or accesses. Shared care records should have a clear policy on how this is done, and all users should be educated about this and have access to guidance.

9. **Hazard Name: Specific data items may be seen by inappropriate users**

Risks: Patient confidentiality breached leading to psychological harm

Generally, the more the data is shared the less control there is over who can see it. The degree of granularity of Role Based Access Control (RBAC) may not be sufficient to ensure that only appropriate data is viewable by other specific users. It may not be adequate to base this on role such as 'consultant' or 'clinician'. What is relevant to a gynaecologist may well not be to an Orthopaedic surgeon.

Trying to police access by limiting access purely by role, i.e. by RBAC, is not sufficient to resolve this problem. We recommend that consideration be given to setting up of the immediate auditing of access to particularly sensitive information, so that at all stages, *all* users constantly ask themselves 'should I be accessing this?' knowing that someone else will inevitably be watching what they have chosen to do.

10. **Hazard Name: Important data not visible to user**

Risks**:** The patient may be harmed because of data not being visible - for example access to data relating to important diagnoses, investigations or treatment might be restricted where the view of record is filtered for a specific purpose or in the attempt to minimise 'unnecessary' data sharing.

Although the application of the GDPR is intended to minimise data which is inappropriately shared, in practice it has created complex stresses and uncertainties for both individuals and organisations who are trying to minimise data sharing but equally, very correctly, wish to maximise the ethical sharing of important data. In particular we were mindful of the recently added seventh Caldicott principle - that t*he duty to share information can be as important as the duty to protect patient confidentiality.*

Practical problems often arise within the NHS because different arms of it are treated as 'different organisations', with potentially draconian limitations on what can be shared. To improve this situation yet remain both ethical and within the intention of the GDPR , consideration should be given to treating the NHS and Social Care as a single body for GDPR purposes. Under such an

approach, any work performed under the aegis of NHS/Social care (i.e. organised and/or paid for by NHS/Social care) would automatically be treated for GDPR purposes as occurring within a single organisation (NHS/Social care), and thus not be affected by GDPR rules about passing on information to other organisations.

11. **Hazard Name: Failure to retain or delete safeguarding records appropriately after the age of maturity is reached.**

Risks:

- Inappropriate retention of safeguarding data leading to psychological stress on the patient.

- Inappropriate removal of safeguarding information leading to continued physical/mental abuse of someone who is vulnerable.

- Legal punishment for the individual/ organisation in relation to inappropriate removal/ retention of safeguarding information .

Health care workers are not clear about their legal and professional responsibilities and duties in this regard. There is widespread uncertainty about the legal aspects of record deletion/retention in a shared medical record where those entries relate to safeguarding. Important data regarding safeguarding may be shared from the source record but the metadata around how long to retain it may be lost, or absent in the first place, or the shared care record may not have an agreed mechanism for dealing with this. For instance, it is not currently part of the *Professional Record Standards Body (*PRSB)'s Core Information Data Model.

The design of shared care records should include a 'retain until' date or 'retain after', where safeguarding data is known to be required to be deleted at some time in the future or retained beyond expected time. Automation of deletion at appropriate date could be considered.

It was felt that there was a lack of clarity over the regulations (both legal and professional) in relation to the retention of records — in particular, after a juvenile, previously subject to safeguarding supervision, has attained legal maturity; and after a patient has ceased to be treated by an organisation.

It was felt that clarity should be sought from the medical and legal profession and then widely disseminated and regularly taught - particularly if any changes to the recommendations have occurred.

12. **Hazard Name: Original document not available**

Legal data may indicate that there is a signed Power of Attorney or a 'Do Not Resuscitate' document, but there is no link to it within the record.

This could lead to legally binding decisions not being followed leading to patient harm and legal action against HCP.

This may occur when the original record stored on a contributing system is not shared or the original record not stored on the system and there is no indication of where it might be stored.

It was noted that the presence of an entry indicating the existence of a document reduces the risk of a document being missed, but does not eliminate that risk. The importance of such forms lies not so much in that they exist, but in the exact details contained within them, and the knowledge that they are indeed the most up-to-date versions.

It was suggested that a central location for legal documents is developed, or alternatively the use of Digital Object Identifiers (DOIs), so they can always be accessed.

Medication

13. **Hazard Name: Medication details not complete or not accurate in a Single Shared Record**

Risks: Patient harmed by inappropriate medication or its delivery

A patient might continue medication which should have been stopped; or does not start medication which should have been started; leading to possible harm. Alternatively, an additional medication is prescribed which causes interactions with existing but not visible medication; or symptoms are not recognised as drug side effects because the new drug is not mentioned in the list of currently prescribed medication; or the dose of the drug visible on screen does not alert the user to the possibility of a relation to a specific side-effect which tends to be dose related.

This hazard was felt to be caused by the lack of ability of a user to change or delete medication issued by another organisation. For example:

- Secondary care prescribes drug (or new drug timing/pack size/instructions) which it wishes to be continued, but GP is unable to edit.

- Community care wish to stop drug prescribed by GP, or amend the dose given, but are unable to edit.

- A drug prescribed by the hospital is not prescribable by the GP, who is unable to re-authorise or amend it.

- GP unwilling to prescribe medication recommended/requested by a hospital consultant or clinic (NB a potentially valid action if the specialist's recommendation clashes with the treatment being provided for a different problem.)

- Lack of clarity over who is responsible for prescribing/initiating/monitoring/discontinuing a medication item.

It was noted that regarding this, SystmOne has a facility to message a repeat prescriber in another organisation, which creates a task to amend prescriptions which that second person originally created/authorised. (However, this may introduce a delay before the appearance of a prescription change in the shared record.) Developing mechanisms in single shared records to prevent re-authorisation of medication until a medication change from a third party is reviewed would mitigate this. One such mitigation would be to add a very prominent flag to a medication item, where a clinician other than the initiator wishes it to be stopped or altered. The flag should ensure it cannot be re-issued without review.

In shared records which are not the prime source of entry, medication is managed in the source system, and this is a mitigation. However other issues arise in updating the medication when changes are made to the recommended medication. When care is handed over and a change in medication recommended this may not be reflected for a period of time in an updated medication record in the source system, leading to the patient taking a regime different to the one recorded. Some medications are prescribed by the hospital only. These can be added to the record of prime entry in another organisation as "prescribed elsewhere" but the use of this facility is both not mandatory, and variable.

To have a single medication record is a laudable aim and the possibility of using a single national central patient medication database should be explored.

This hazard is likely to occur when there is a lack of clarity over ultimate responsibility for prescribing, when there is a difference of professional opinion; clarification at national level of the relevant responsibilities here regarding this should be sought as a matter of principle.

Record contents

14. **Hazard Name: Multiple Entries of same data item**

The same event may have been recorded by different organisations or by the same organisation multiple times, leading to two or many entries of coded data for that event. This may occur because:

- An HCP adds an event or diagnosis code as reason for encounter…

- … or an on-going review or does not use episode notification correctly.

- A data item might be coded to one level of granularity by a specialist, and to a lesser level by the GP, and then both entries are displayed in the shared record.

- The same event may be recorded with different dates, especially if one date is the date of first symptom occurrence and the second is the date of a letter/ date of diagnosis.

- An individual item may need to appear under two or more headings (e.g. blood pressure). There needs to be a mechanism by which a single entry can be made to appear under several different headings.

In non-single shared records, there is likely to be a de-duplication process, which will tend to mitigate this, but may add the hazard of losing data. Consideration might be given to introducing de-duplication to single shared records, or at least providing a de-duplicated view of the data. The meeting discussed designing ways of displaying similar data items, and/or flagging that there is a similar one already in the record when entering a code.

Education and training in the use of EPRs is needed, to ensure that users understand the importance of only entering events once; with an appropriate use of coding and date; only after visually checking that the diagnosis hasn't already been entered; and that they understand the use of episodicity.

Record Structure

15. **Hazard Name: Structure of record may prevent important information being found.**

The detailed way in which individuals or organisations choose to lay out the record may prevent information being seen (or easily discovered). Ambiguity over the laying out of the record also creates uncertainty over where specific entries should be placed. The importance of specific pieces of information may therefore be misunderstood. This can lead to important data may be missed or misinterpreted, leading to patient harm.

The causes of this are thought to be:

- where the record is not sufficiently structured, so there is simply too much data and important facts may be overlooked

- the structure is unfamiliar and it is not clear where to find information (this applies particularly in unfamiliar shared records with many section headings)

- The structure of record may be restrictive, with no appropriate heading for data to be placed under…

- …or because the structure of the record is repetitive/ambiguous and there is no single clear place to put an individual item…

- … or there are several different places (quite fairly and logically) to put the information (eg. BP under CVS, diabetes, eyes...)

- There may be an inability to suitably filter the View for current needs of the user

- The user may be prevented from curating data entered by another user…

- … or the record may not be not curated by anyone due to lack of time; or recognition of the importance of curation.

There has been extensive consultation on the structure of the record by the PRSB in building the Core Information Standard, but it is not clear whether this is enough. In particular it consulted on what sections users wanted to see and not about the structure and relationships of that data in the core systems.

This can be mitigated by allowing different ways of laying out and viewing the patient record that can be selected and created by different users or groups of users, organisations or specialists. It needs to be ensured that users are involved in design of these alternative layouts and that adequate initial and on-going training is provided in the use of the EPR.

The Shared Record Professional Guidance paper states

"The design of shared records needs to take account of this problem. Some potential recommendations, which might reduce the chance of this kind of problem occurring, are to ensure that:
1. Representatives of all health professionals using the shared record are involved in defining the headings under which data items are listed
2. Data items can appear under multiple headings as necessary
3. The names of the headings are as explicit as possible to as many professional groups as possible, to reduce ambiguity
4. Patient involvement in deciding headings could be considered as an option if no agreement can be reached between professionals. This would also help patients to navigate their own record, an important goal but one which is outside the scope of this review."

16. **Hazard Name: Loss of data context and/or provenance**.

This may occur where the context of data (the way it is recorded in the logical data model) in the contributing system is lost on sharing, or it is not clear where the data has come from. This can lead to important data being missed or misinterpreted leading to patient harm. ('Patient improved' is of little use if it isn't clear which symptoms are being referred to.)

This problem may be caused by an inability in shared records where data is shared in from multiple sources to fully replicate or integrate the data models of all contributing systems. Misinterpretation of dates attributed to a data item e.g. date of *entry* by comparison with date of *event* may also cause this hazard.

The group felt it was important to ensure that the logical data model allows context and provenance (especially around use of dates) to be preserved as much as possible when data is shared with another record and that it is important to ensure the relevant data in a problem is shared where it supports a narrative or a diagnosis. Reference was made to the Shared Record Professional Guidance paper comment that ***"Data becomes information only when the context of use is known"***.

Referrals

17. **Hazard Name: Referral Information is ignored by recipient**

There is a risk that the referral Information is ignored by the recipient either because too little information is shared and it is of poor quality or because too much is shared by a data dump from the computer system leading the recipient to devalue the data shared.

In *Single Shared Records*, referrals may very appropriately be made internally within the system, where data dumps add no new information and simply cloud the issue. However, in some circumstances this may lead to proper attention not being paid to truly important data in the referral, leading to misinterpretation of need or inappropriate care

As a result, the patient is thereby harmed physically or psychologically.

The causes for this hazard include:

- performing a data dump from all or part of the record, rather than carefully selecting/quoting appropriate information.
- or, if using same Single Shared Record as the recipient, failing to stick to just a brief, concise statement of why a referral is being made which refers to salient findings already within the joint record.

A mitigation was noted to be the PRSB clinical referral standard, but it was felt that it would be beneficial to have an agreement around what best practice is, when referring using different systems, together with ensuring that users are educated about it and can find guidance to support them.

Responsibility for care

18. **Hazard Name: Unclear who is responsible for different parts of patients' care**

There may be an inability to tell from the shared care record who is responsible for a particular part of the patient's care. This may lead to important care actions not being carried out by the intended HCP, leading to patient harm.

This may be caused by an overlap of areas of care; and of transfers of care where there is no clarity in record of who has agreed to be responsible or no standing national or local agreement on who is routinely responsible in such cases. It might also arise where there was an introduction of a system to hand over tasks with no agreed standards on appropriateness.

It was noted that there were some recommended professional behaviours already in place, but these have not been uniformly adopted, updated, or monitored.

The group noted that there is a lack of clarity over responsibility for care actions, particularly at interfaces of care. Agreeing who is responsible is particularly important over dealing with the results of investigations, reports and unexpected incidental findings. These should be agreed by the professions, nationally adopted, and their use monitored. Consideration should also be given to mechanisms to embed formal hand-over in system design, allowing for acceptance or rejection of the request. (See Assessment, Discharge and Withdrawal FHIR model.)

Safeguarding

19. **Hazard Name: Safeguarding information not found, or data is inaccurate, incomplete, or inaccessible.**

Important data about safeguarding is missed by user or misinterpreted and as a consequence a patient is put at risk of harm or abuse.

The causes of this might be:

- the absence of a special shared area within which to place safeguarding information.

- the failure of some or all the contributors to the joint record to place safeguarding information in the correct places.

- the failure of some of the users to look at these designated safeguarding areas.
  Another issue noted was where a user does not have appropriate RBAC to be able to see the information.

In one Single Shared Record (SystmOne) there are pre-defined sections within the shared record for depositing safeguarding information. Data sharing in these areas is specifically and deliberately *not* subject to the control of the patient's/carer's consent mechanism, in order to ensure that the contents of these areas cannot be suppressed inappropriately by patient or carer.
The correct use of RBAC, with appropriate granularity, is required to ensure that these areas are/aren't visible to relevant health care workers (who may not necessarily be healthcare practitioners: clerical staff may well need to know that safeguarding concerns exist, even if they are not permitted to view all the details).

The group recommended that there are clearly identified sections of the record for recording and viewing safeguarding information of various types. It also recommended that users are educated in

how safeguarding information is displayed and that instant audit alerts are set for sensitive data items as this was felt to be better than using RBAC which could stop vital information being accessed.

Secondary uses

20. **Hazard Name: Inappropriate data produced in a report about an individual patient.**

A report might contain data which, from a legal point of view, is inappropriate, either because there is too much data included or too little for that purpose as measured against legal and professional guidance.

There may be uncertainty on what data should or should not be shared from a shared record when creating a legal report or subject access request (SAR): for example, do they contain the entire shared record, or only the part entered by the organisation from whom the SAR has been requested.

There is legal advice already on this, but it is not well-understood, nor easy to look up with certainty.

There is a need to develop standard recommendations and instructions about the legal aspects of creating medical reports in relation to confidentiality, GDPR etc— reports for patients; referral letters; insurance reports; safeguarding purposes; SARs; and court reports. The structure and content of these recommendations should be professionally endorsed. These agreed instructions need to be readily available from a single government website.
Based on this, organisations need to create and maintain ongoing tuition about the legal and practical technicalities of creating reports in their organisation, and when using their data, and data emanating from other organisations using the shared record.

Teaching and implementation

21. **Hazard Name: Lack of training and education in use of EPRs**

There is a lack of training and education in the use of EPRs (EHRs), especially in shared records, both generic and system-specific. This applies to all levels of medical education. The consequence of this can be poor quality records leading to important information not being accessed or not available when needed and the patient suffers harm as consequence.

There was felt to be a lack of consistency in achieving permanent solutions, caused by:

> • Lack of decision-making nationally about matters of professional behaviour and principle (e.g. responsibility for prescribing; or for follow-up of abnormal test results)
> • Failure to get national/local agreements over which codes to use/avoid in specific situations (especially in relation to the QOF)
> • Failure to clear up legal problems/anomalies (e.g. re GDPR)
> • Failure to teach the final conclusion of these matters consistently, widely and regularly enough
> • Lack of consistency over putting solutions into place across the whole of the NHS estate.

It was noted that there is some teaching, but it is often very basic, often only done at the beginning of the use of a piece of software, not followed up, not performed regularly, and doesn't allow users to develop a deeper understanding around the use of the software; often new entrants aren't actually formally taught.

The group recommended **On-going** support and training in the use of systems (and not just induction of new staff or when the system is initially deployed); and better training throughout clinical education in all disciplines, in the use of EHRs and the importance of keeping high quality electronic records.

Terminology

22. **Hazard Name: Incorrect or inaccurate SNOMED CT concept**

An SCT concept in the record is incorrect or inaccurate or loses specificity by being higher in the hierarchy.

The risk is that important data may be missing, leading to patient harm. *Computer-based decision support may be triggered inappropriately or not at all, leading to failure to give best care*. There may be financial implications for the user of the record or another organisation if quality payments are based on inappropriately recorded data.

The causes of this are:

• Different levels of clinical expertise may lead to different levels of recording data.
• Lack of education and training for users of the system in SNOMED CT
• No constraints on SNOMED hierarchies
• Non-QOF code added by another organisation, leading to failure of decision support.
• Not all organisations are using SNOMED CT; data may still need to be mapped from another terminology, leading to errors.

SNOMED is now mandated throughout the NHS, which will improve consistency. Consideration might be given to constraining the use of SNOMED hierarchies in different areas of the record to improve data quality.

There should be agreed and mandated standards for record-keeping across agreed care pathways, mitigating for differences in systems. Education and training in use of terminology throughout medical education is needed to ensure there is understanding of the appropriate use of concepts in different hierarchies, especially the use of concepts in the Special Context hierarchy which include such things as Family History, *and which may not themselves refer to the person who is the subject of the record*. In addition, there is the potential for concepts added by one organisation to affect financial and clinical targets (such as the QOF) in other organisations. A common example is where a diagnosis code is added for a second time (suggesting a new diagnosis) instead of a treatment code; or a procedure concept such as 'Flu Vaccination given' rather than a concept indicating a third party had carried out the procedure.

Data Quality audits and feeding back to users would be a useful tool to drive up the correct use of the terminology. A one-off exercise was undertaken, auditing the use of Read codes in the IM&T Direct Enhanced Service (DES)in 2006, which exposed significant misuse of codes, such as adding "Meningitis" diagnosis codes instead of the vaccination code.

23. **Hazard Name: Inactive concept or local code shared to the shared record**

An active or local concept in the contributory system becomes inactivated in the shared record.

The consequence of this is that important data may be missing leading to patient harm; or decision support may be triggered inappropriately or not at all. Both these can lead to failure to give best care.

Different organisations using different editions of SNOMED CT or not updating synchronously may lead to an active SNOMED concept becoming inactive in the shared record; or if organisations use their own SNOMED CT namespace and generate their own concepts. The shared record will not be able to understand these in a structured manner. Both of the above could lead to an alert not being triggered, and consequent patient harm.

The UK Standardisation Committee for Care Information (SCCI) standard does require the use of UK edition. The version of SNOMED used in each contributing system should be part of the metadata included with the data, so that the manner in which it behaved in the contributory system can be understood. System suppliers need to ensure their local codes are mapped to SNOMED equivalents as they become available. Generally, the use of local codes should be deprecated.

24. **Hazard Name: Post co-ordination of SNOMED or qualifiers allowed by some organisations contributing to record**

A post-coordinated SNOMED term or a SNOMED term with a qualifier could be received but not understood by the shared record and meaning is lost.

As a result, data may be incorrectly interpreted leading to patient harm, e.g. in relation to certainty of diagnosis, laterality and possibly negation.

This would occur where there was adoption of post-coordination, or use of qualifiers by an individual organisation without considering the shared record consequences. i.e. The shared record cannot handle post co-ordinated concepts, but the contributing organisation does.

Consideration should be given to this in developing shared records.

Usability

25. **Hazard Name: Important data not found by user**

If the usability of the system is poor for some or all users, making it difficult for them to use the system effectively, important data may no be found.

This can lead to data not being available when a HCW needs them to make diagnosis/adjust treatment accurately and patient harmed or to investigations being repeated, which are unpleasant and inconvenient for the patient, and may create delays in diagnosis, waste resources, block resources for others.

The causes of this were felt to be:

- Poor interface, unclear headings
- Not clear which section to find data in, or place data in
- Data tsunami leading to important data not being easily visible.
- Incorrect or poor data being entered or data not being entered.
- Poor usability of system may lead to lack of user engagement with/ownership of the system leading to devaluation of shared record.

Different organisations and even different users will want to view different data in a summary. Therefore user-configurable views of the data are important; and users need to be involved in the design and its updates, and allow customisation to accommodate preferred workflow.

Vaccine history

26. **Hazard Name: Inaccurate or incomplete vaccine record**

The vaccination history is inaccurate or incomplete leading to a vaccine dose not being given or given inappropriately.

Separate IT systems may not all be connected into the shared record or the record may be based on patient or carer recall in a particular record e.g. inaccurate recall of vaccine or date or cardinality Vaccination history in certain records (such as the Maternity Care Record) may be restricted to specific time frame or specific vaccines.

Everyone connected with the immunisation and vaccination programmes should be properly trained to ensure that all contact and work performed is fully entered into shared patient records — but only the once! — and in particular, using administration and reminder codes so as carefully to distinguish between the plans and preparations for immunisations, and the immunisations themselves.

The provenance of the records should be clear as well if effective construction of a single vaccination record is to be created.

Value sets

27. **Hazard Name: Value set prevents correct data appearing in correct place**

Value sets are used to constrain many fields in the shared care record. If they are incorrect/incomplete or not kept up to date the appropriate data may not appear.

The maintenance of large complex value sets can be time consuming and expensive. Ownership of any value sets should be clear.

There was agreement that changes to the externally-derived content of Composite Shared Care Records (CSR) should be only made in the contributing source's system by its owners and then carried through into the CSR itself, although they may have been prompted to do so by the CSR owner.. Furthermore, with any shared care record, agreement should be sought at the outset on when and how data can be edited, and what was the appropriate way to edit it, so that the provenance of any change can be ensured and the reasons for change noted. Users need to be educated about this & training and guidance should be available.

A general concern/question was raised about the preservation of an audit trails when a system that has individual systems cease to exist and in particular if they had contributed to a shared record ceases to exist. This principle applies to all EPRs and the group recommended seeking a that a national solution for this should. be sought.