Sharing Digital Records with Safety and Quality

Introduction

"Sharing systems is not the same as sharing data" – this informatics aphorism is examined and proposals made on features needed for safe and effective nationwide systems for sharing Electronic Health Records.

1 **Data security and access control.**

The sharing of data beyond its original clinical context can create new risks arising from poor quality or inappropriate content in the data shared, and from inappropriate accesses. There are major health benefits for some patients whose data is successfully shared, but there are major disbenefits for other patients whose shared health data is of poor quality or accessed wrongly. So sharing systems require these functions:

a) Access Controls on which data is shared, how it can be viewed and by whom,
b) Quality Assurance of any data that has been shared.

a) The primary use of e-health information-sharing is between Primary and Secondary Care In this context, an initial proposal from CfH was for default sharing to the Shared Record, but GPC and RCGP have confirmed preference for default no-sharing of clinical data (also known as opt-in) to ensure patient control of information sharing in a joint "Act of Publication" of Quality-assured data to the Shared Record . Scotland's Emergency Care Summary shares a highly reduced subset of data that is of high quality - only demographics, recent prescriptions and recorded ADRs – and the risk of inappropriate access is minimised by patient-controlled direct consent for one-time use in each care episode.

CfH have issued a Care Record Guarantee, under which Access Control is proposed by a "Sealed Envelope" system. .If the networking of Digital Records were uncontrolled, the Shared Summary record would continuously update from the GP system data that should be restricted. However, a patient with privacy issues supported by the Guarantee may expect the same security for their record regardless of which part of the NHS is at that time responsible for them, as determined by the patient's clinical journey. So the security status must itself be inter-operable, and systems designed to use it wherever that data is shared.

The range and scale of privacy issues is a concern. Issues of Identity Management include some that are legally enforceable e.g. for adoption or gender change histories, for those formally on Witness Protection schemes; and for many thousands who are informally hiding under aliases or at secret addresses e.g. from violence. The management by "stop-noting" of demographic data is under review by CfH. Other issues arise in the content of Data: that specified data is known only to specified users, or unavoidable professional relationships e.g. rural practice; or references to 3rd-parties; or ad-hoc requests by patients to restrict access to specified clinical items.

However, Access Controls for sensitive data are now standardised in all 6 Dutch GP systems., and experience in Holland suggests that the scale is not large. However it is unpredictable which data may be requested by a patient for privacy restrictions e.g. an old address for a victim. We also understand it is partly supported by iSoft's Synergy (and Meditel before that) - but not fully by other systems e.g. EMIS and Vision can support partial display/hide switching only, as may GPASS Clinical Phase 2. We are thus currently unable to assure patients that their sensitive data can be handled reliably within our practice systems, or if the pt. moves to another practice system – which may be across any UK Border.

Digital records exist in 2 main formats: the Native e-Record, and the Document-based e-Record, containing clinical data in original narrative form, usually scanned. Both need access controls, and to re-integrate the record these also must inter-operate. For example, when The State Hospital at Carstairs introduced paperlight working, security was the first consideration e.g. detailed access controls to the individual user level for each document. This functionality was not thought to be available from the usual systems used in GP including Docman, (procured nationally for Scotland) – so they use Docuware, a German product for general business use.* This requirement they considered exceptional – but this requirement may be shared by a few patients in many other care settings. For example, even forensic psychiatric patients eventually return to a GP practice, where they have a right to appropriate health data being transferred with safety and quality, but with protection of forensic data.

Sharing data for such Secondary Uses as for epidemiology and registries raise similar issues, for which the different context offers different solutions. In summary, security is a fundamental for all shared Digital Record systems and must function wherever sensitive data is accessed across the whole data-sharing environment. The difficulty of predicting in which circumstances which data may be sensitive demands that interoperable access controls be available to all data system-wide.

* However, Docman does support a 10-level access index to link a user to a document, so some security functions are already in place.

b) **Quality Assurance** of the data shared also needs to be shareable with that data. On receiving data shared by unknown others from an unknown clinical context, a judgment must be made by each clinician on its quality, and this needs metadata (data about data) to form such a judgment on its "Provenance". Both native and document-based records can show provenance by audit trails, though some current systems' audit trails are not easy to use in a live clinical scenario.

Unfortunately native records use proprietary databases often configured for each installation, so there is no foreseeable way to support interoperable transfer of audit trails between installations, even when the native format is the same. For document-based records the audit trail was similarly incompatible between installations – but Docman v7 now supports exchange of an interoperable same-system audit trail, thanks to the mandatory use of a standard National Index for filing document-based records in Scotland.

Authorship is a major element of provenance, and is usually identified as the logged-on user, but systems currently vary in how this is presented, or secured from change, either intended or tampering. Pilot GP2GP demos have found anxiety by receiving clinicians on the provenance of the data being imported, with request for clinically usable indications such as colour-coding for authorship by name or job title. A more general method of showing provenance is by displaying such details as if properties e.g. via right-click, or on a menu.

Work area 1:

- Identity management in demographic services need review to support UK - interoperability
- Access controls for sensitive data should operate both in native- and in document-based systems, for so long as records that are hybrids of native + document Digital Records are in parallel use.
- Quality Assurance should include provenance, including authorship.
- Provenance should be clinically usable, for example when provided by reference to audit trails.
- Both Access controls and QA need to be transferred as metadata with the clinical data to be shared
- Systems need to be designed to be interoperable for this metadata.

2 **Document-based (scanned) e-records** have a central role as enabler of Digital Records in the transitional phase between paper and full native e-records – and this raises other security issues:

For legal admissability the processes of scanning and document management are defined in the BSI's BIP0008. The security demanded of images is that they should be in a near-incorruptible format such as TIFF v4 or above. But other formats are widely used e.g. Acrobat .pdf, and .jpg formats in creation or imaging of clinical documents. Both the latter are easily "edited" - if not quite so easily as Word files, which are themselves widely used for original documents sent by email. Further, although accesses and changes are recorded in an audit trail, these are not transferable between systems. While the image files are encrypted at the file-system level, anyone with access by password, and an intention to use a little technical knowledge that is not deterred by the risk of detection in an audit trail, can access them to tamper or copy.

Tamper-proofing can be partly supported by the access controls inherent in Managed Server/Thin Client environments. Tamper-evidence can also be implemented by frequent digital "hashing" of the records, which may also be facilitated by Centralisation of data storage. However, currently there are thousands of e-records being transferred with uncertain physical security or access controls.

Work area 2: physical security of file-types of all e-documents in clinical use should be reviewed.

3 **User authentication**. The security model also depends on this. In normal clinical settings it is informally provided by small working groups with personal recognition in the workplace of a user, and the clinical access to Scotland's Emergency Care Summary includes this in its security model.
At TSH Carstairs user authentication is augmented by physical access control such as video surveillance.

In England CfH is improving authentication by adding Role-Based Access Control by use of physical tokens, adding "Something you have" to "Something you know." In England these are currently a smart-card for each healthcare worker, requiring a dedicated reader. There may be other technologies - e.g. generic USB flash disks can hold encrypted keys, and can also hold personal data such as health data - which for ~1m. NHS workers would most conveniently combine both functions.

However 250,000 patients migrate annually between 4 UK nations with the same security needs for their records, so support for the same security functions is needed UK-wide. Having authenticated each user, the access privileges assigned to each user need to be correct wherever shared data originated, so that a record with sealed-envelope data, moving with the patient anywhere in UK, is similarly secured.

Work area 3: UK-interoperability of security systems also requires to be addressed.

4 Digital record systems and architecture

We have discussed some practical issues raised by the current systems in document-based- and native-system digital records. In trying to define an agreed future state in digital systems, however, there does not seem to be an agreed set of components to support their safe and effective sharing in a national system.
A high-level description of such a system may feature some of these components:

Messaging – to support transfer. The HL7 v3 RIM international system seems to be the de facto standard.
- it is now considered unsuitable for data storage as had been proposed

Architectures – to support function in different contexts.

- CDA – an earlier HL7 system that includes an architecture for document-based records.
- OpenEHR – an international system of archetypes designed to structure native records.
- National Datasets – the NCDDP set is wider but less detailed than the OpenEHR set of archetypes

Terminologies - to support computability.

- Read – these established codesets are in several versions with complex compatibility issues
- SNOMED CT – this vast library is internationally agreed as the future, and much work has been done to map Read to this. However it is implemented to date in only one usable s/w, by Healthysoft.

However, text is the original "terminology" and has many benefits - for example:

- codes can degrade to human-readable text;
- it supports clinical narratives on which most clinicians depend, and which are mostly uncodable
- it supports modifiers safely e.g. the very dangerous negation that is essential to process accurately.

It is suggested that text support is mandated in all clinical systems for its safety features

Software products

- Clinical systems - each have proprietary data models of native records for specialist purposes
- Generic Clinical System – this toolkit uses generic data models such as the NCDDP datasets covering most common items. However the software products will be proprietary native systems.
- Document-based record systems – similarly for documents in generic formats, linked in proprietary databases. Text support is intrinsic.

It is unlikely that the issues in selecting components and making these inter-operate to an agreed future standard, or any implementation of such a future standard, will soon be resolved at an organisational level.

An alternative approach is to define the metadata required for safe and effective sharing, and to focus on the processing of clinical datasets in those clinical areas where sharing of data is most useful. This uses the feature that at machine level it is all just "data" and metadata is natively processed just as if it is clinical data. Each component as above can then process and add value to the data in its own way. Thus:

Clinical data:	
1. native-system data	- using codes and text linked in proprietary databases.
2. document-based data	- includes scanned and misc. other e.g. emails, photos, ECGs.
Metadata	
3. QA / provenance / attestation	- as discussed above
4. security status of data / users	- as discussed above
5. view options, controls	- arguably a subset of the above
6. e-record structure integrity	- e.g. tracking data/manifest for transfers of hybrid e-records
7. freetext support	- safety feature to be embedded wherever clinical data is shared
8. workflow links	- process tracking e.g. action owners, diarising, audit trail
9. financial	- to support joint working with other providers
10. location pointers	- support future web-distributed/decentralised architecture
11. decision support	- e.g. relation of data to SIGN, NICE guidelines

These metadata classes are in a suggested order of priority.

Work Area 4:

- Prioritise those clinical areas with maximum benefit for e-record sharing.
- Identify any new metadata classes and agree those required in these clinical areas.
- catalogue the current support for agreed metadata classes in current and known future systems.
- Prioritise and Fill in the gaps.

Colin Brown
GP Paisley; Director SCIMP colin.brown99@nhs.net