Sharing Digital Records with safety and quality

Introduction
"Sharing data is not the same as sharing systems" – this aphorism is examined here and proposals made on how to construct a safe and effective national system of shared Electronic Health Records.

1 **Data security and access control.**
The sharing of data can create new risks arising from poor quality or inappropriate content in the data shared, and from inappropriate accesses. The health benefits to those patients whose data is successfully shared must be compared to the disbenefits for other patients whose health data is of poor quality or is wrongly shared. Shared Digital Record systems require these major 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) In 2005 CfH proposed a hybrid consent model featuring default sharing for most global clinical areas and default no-sharing, also known as opt-in, for some others e.g. mental health and sexual health. However clinicians were unhappy about any default sharing, except for the highly reduced subset of data in Scotland's ECS project, which shares only demographics, recent prescriptions and ADRs for use in a single Point-of-Care episode. GPC and RCGP recently endorsed a position of default no-sharing of clinical data/opt-in to ensure patient support for the safety and quality risks of sharing clinical data.

If there were no such controls, the networked Digital Record would have continuous updating of the Shared Summary record from an insecure GP system holding data which should have been determined to need restricted access. A patient anxious about their record will not be reassured if the local system doesn't support the same access controls that is promised on the Shared Record. Further, patients will learn to expect the same standard of security for their records regardless of which part of the NHS is at that time responsible for them. The access status must itself be shareable, and systems designed to use it so that it can be implemented wherever that data is shared.

Full access controls for sensitive data are to be standard in Dutch GP systems, and currently implemented in 4 of the 6. We also understand it is partly supported by iSoft's Synergy (and Meditel before that) - but not fully by other systems e.g. InPS' Vision can support partial display/hide switching only, as will 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.

The scale of the problem is a concern. Examples of sensitive data will be found in people with adoption or gender change histories, on witness protection schemes, hiding from violence, or in unavoidable professional relationships such as staff being patients of a rural practice. 3rd-party data also needs special handling. Further unpredictable requests are often made by patients in Primary Care, that some data is known only to one user. Experience in Holland, suggests that the scale is not large, but also that it is unpredictable which data may be requested by a patient for access control e.g. an old address for a victim. So the functionality may need to be present for all clinical data in every system, though occasionally used.

The digital record has 2 main parts - the Native Record as above, and also the Imaged Record, containing clinical data in narrative form: both need interoperable access controls. When Carstairs State National Hospital went paperlight, security was specified that may be thought to be exceptional - but may be no greater than is required for some patients elsewhere. Even forensic psychiatric patients eventually return to a GP practice, where they have a right to appropriate health data being transferred. Carstairs approached the issue from the POV of security first, with detailed access controls to the individual system user level, for each document. This functionality was not believed 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. However, Docman does support a 10-level access index to link a user to a document, so some security functions are already partly in place.

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 data may be sensitive suggests that access control be available to all data system-wide.

b) **Quality Assurance** of the data shared also needs to be shareable with that data. "Provenance" refers to the meta-data required to support the judgment that must be made by each clinician on the quality

of data shared by unknown others. Both native and imaged record systems can show provenance by audit trails, though current systems' audit trails are not easily usable in live clinical scenarios.

Unfortunately for native records there is no foreseeable way to support interoperable transfer of audit trails between local installations, even when the native format is the same. For Imaged records the audit trail is similarly incompatible between installations – but Docman now supports exchange of an interoperable same-system audit trail in v7, depending on mandatory use of a standard National index for its filing system, as now used by Scottish paperlight practices.

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:

- Access controls for sensitive data should operate both in clinical systems and in document-scanning systems, for so long as hybrid native + imaged Digital Records are in parallel use.
- Quality Assurance should include provenance, including authorship.
- QA should be more clinically usable than 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 **Imaged documents** have a central role as enabler of Digital Records in the transitional phase between paper and full native e-records – and this raises other issues:

The security demanded of images for legal purposes 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. Further, although accesses and changes are recorded in an audit trail, these are not transferable between systems. While the files currently used in document-imaging are encrypted at the file-system level, anyone with access to them via the password, and an intention to use a little technical knowledge, and if not deterred by the presence of an audit trail, can tamper or copy them.

Tamper-proofing is 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, meanwhile there are thousands of e-records being transferred with indeterminate physical security or access controls.

Work area 2: physical security of file-types of all document images 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 of users; at Carstairs user authentication is augmented by physical access control such as video surveillance.

This is being upgraded in England by use of physical tokens, adding "Something you have" to "Something you know" – as authentication is improved by use of both. 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 across 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 by whatever means, the access privileges assigned to each user need to be correct for shared data wherever it is originated, so that a record with sealed-envelope data, or the related Scottish "break-glass" audit trail, moving with the patient anywhere in UK, is similarly secured.

Work area 3: UK-interoperability of authenticated-user privileges also requires to be addressed.

4 Digital record architecture

We have discussed some practical issues raised by the current products in scanning and native-system digital records. In trying to define an agreed future state, however, there does not seem to be an agreed architecture for data structures in native systems to facilitate their integration into a national shared system. There are in Scotland several candidates:

- HL7 – an international system designed for messaging
- CDA – an earlier HL7 system that includes text documents.
- OpenEHR – an international system of archetypes designed to structure the native record
- National Datasets – the NCDDP set is wider but less detailed than the OpenEHR set of archetypes
- XML – can this universal data-handling language be used to define standards?
- Generic Clinical System – this includes a set of data models covering most common items
- Other clinical systems - each have their own ad-hoc data model for restricted purposes

It is unlikely that the informatics and organisational issues behind joining these models will ever be resolved.

An alternative approach is to define what data about the clinical data – known as metadata - are needed to support safe and effective sharing and to ask data or datasets arising from each architecture progressively to include it. This depends on metadata support being a generic function of all IT systems. Thus:

Clinical data:

1. native-system data
2. imaged data - includes scanned and misc. other e.g. emails.

Metadata

1. QA / provenance / attestation - as discussed above
2. security status of data / users - as discussed above
3. view options, controls - arguably a subset of the above
4. freetext support - safety feature to degrade to human-readable text
5. workflow links - e.g. action owners, referral tracking
6. e-record structure integrity / manifest - e.g. Docman National Index, tracking data for transfers
7. financial - to support joint working with private providers
8. location pointers - support future web-distributed architecture
9. decision support - e.g. relation of data to SIGN, NICE guidelines

These metadata classes are in a suggested order of priority.

Work Area 4:

- agree the metadata classes from those suggested above
- catalogue the current support for agreed metadata classes in current and known future systems.
- Prioritise and Fill in the gaps.

Colin Brown
GP Paisley; Technical Director SCIMP

colin.brown99@nhs.net