SBAR Analysis | GP records on Removable Media

1.1 Situation

Some medical records (often, but not exclusively, from outside NHS Scotland) are being received on storage media such as optical discs (DVDs/CDs) and occasionally even magnetic media such as floppy discs and solid state drives. These media are included with the A4 or Lloyd George paper records that are sent to practices via PSD when a patient registers with the practice. Similarly, when a patient moves practice the records on these media must again be shared with the next practice. This could be achieved by extracting the documents and files from the original media and including their information in the patient's medical record in the GPIT system or in the document record in Docman. PSD will not accept original media, however, meaning practices may find they have inaccessible and un-shareable records.

It is not uncommon for practices receiving these media to be unable to read them. This may be because the access has been password protected or the disc encrypted in some way, with the original key or password now lost. The originator of the media may not be clear, so it may be impossible to track down the required passcodes to access the data. It may also occur where no suitable media reader is available – floppy disc drives are now very uncommon and most practices will not have one available.

It is possible that even once security and device obstacles have been overcome, the data may be unusable because it is corrupt or not in a format that will allow it to be re-used. It may not be human-readable, if sent as an application or code specific to an application.

Practices operating completely paperless, with scanned historical records, face particular challenges with these types of media if they cannot extract the records and import them to their records archive for the patient, onto Docman.

This paper is provided for advice and to help guide decision making, but is not intended to be comprehensive to meet all possible scenarios, and does not represent NHS Scotland policy for this issue.

1.2 Background

Storing and then sharing medical records from general practice on storage media (optical / magnetic / solid state) is a practice that has been employed in an often bespoke process to avoid having to send large volumes of paper records when patients transfer between practices. This was primarily a practice in NHS England and is described in the DoH Good Practice Guide for Electronic Records 2012 (copied below).

Backscanning project in Greater Glasgow & Clyde HB has identified this as an issue.

1.3 Assessment

There is clearly a risk to records integrity if the data on the media cannot be read and stored to the patient's NHS Scotland EHR on the GPIT system and Docman. There maybe clinically important information on these media which could materially affect patient care.

Nevertheless, if the records cannot be accessed with reasonable attempts to do so then there is no further action possible and the records are effectively lost. The clinical risks associated with this are no different to the loss of any other paper or electronic record, and currently

although the GPEHR to Docman Transfer process is recommended in NHS Scotland there are still instances where the records are not sent or received with subsequent loss, in the new practice, of the previous information.
Practices can mitigate these risks in the usual ways, by clarifying history gaps with patients and asking directly for any health critical data such as medication adverse events or significant past or ongoing illnesses. Managing the risks of records gaps and poor quality records, as well as incomplete or unclear histories from individuals, are part of usual GP processes.
What is required is a process to demonstrate that all efforts have been made to access the data on the media, and if this fails an agreed process for handling the media thereafter.

1.4 Recommendations

Practices receiving storage media containing records should try and access that data and then import it in its entirety into the GP IT system and Docman, as appropriate. Once all data has been imported the media itself should be destroyed. It may be that the data on the device has already been so imported by a previous practice, but that they omitted to destroy the storage media. Where the media can be read, the patient's current record should be checked before importing the files to avoid duplication where this is the case.

1.4.1 Devices

1.4.1.1 Floppy discs

If no floppy disc reader is available in the practice, this should be referred to the GP practice's IT support via the Health Board for assistance.
USB floppy disc drives are still readily available to purchase, but permission to use such a device may need to be obtained from the Health Board so they should be consulted in the first instance.

1.4.1.2 Optical media

If the practice does not have a compatible CD or DVD drive on a local machine that is able to read the media then again this should be referred to GPIT support at the Health Board.

1.4.1.3 Solid State media

In most instances practices will have PCs with USB ports that will allow these devices to be read but again, in the event of problems, the GPIT support should be contacted.

1.4.2 Security

1.4.2.1 Antivirus precautions

Practices must consult with their local Health Board's IT department for policy and procedure advice before loading any received media onto their practice's computer system.
Practices should of course assure themselves as best they can of the provenance of any received media.

1.4.2.2 Passwords and encryption

Some media may be password protected or encrypted, or both.
Generally, access will be possible if a password key is available, but this may have been lost during the multiple transfers of the record.
Where this seems to be the case practices should put some effort into trying to obtain the passwords. This will of course only be possible where the originator of the media storage is clear. If an identifying practice or sender for the media is found then they should be contacted, if possible. If they are unable to provide the password, as it is not available to them, or they are not contactable then, in effect, the record is unusable and therefore lost.

If the originating practice is still available then a formal request for the password should be made in writing allowing 28 days for a response. In the event no response is forthcoming then the practice can reasonably assume the records are lost, and manage as below.
The ICO would expect practices to make reasonable efforts to access the data, and our opinion is that this would include attempts to contact the originator for the required unlocking codes.

1.4.3 File format issues

The data may be in a format that makes it unreadable, or in a format that is not compatible with new records storage such as Docman.
If the data is in an old or legacy format rendering it unreadable on current IT in the practice then the Health Board GPIT support should be asked for assistance. Rarely it may not be possible to access this data at all, as software applications may no longer be available. The practice should not make this decision, but take advice from their HB. If this is the agreed position then the records should be treated as lost, as below.
If the data is in a legacy format, but can be read, it may need to be converted to a new format to allow it to be imported into Docman or the GPIT system. There is no single solution to achieving this and, if the practice is unable to resolve the issue in house, HB advice should be sought.

1.4.4 Lost records

Records on portable media may be considered lost where:

- Despite reasonable efforts by the practice no device is available that can read the media
- Despite reasonable efforts by the practice the access codes for a password or encryption protected media have not been able to be retrieved
- Despite reasonable efforts by the practice the file format of the data on the portable media is now legacy and no currently available software will enable it to be read or converted to a modern format

In this case the practice, as the current Data Controller, will have to inform the patient. They should explain that a previous practice has stored some of the patient's records on portable media but that all efforts to access it have been unsuccessful. This may constitute a Data Breach under the DPA and GDPR if the patient is materially affected by the loss of these records. The practice that has identified the issue is not the liable party, however, and by following the guidance herein would be compliant with their responsibilities as Data Controllers. It would not, however, be acceptable simply to destroy the media concerned without informing the patient.
Practices should also make efforts to fill in the gaps by direct inquiry with the patient, to mitigate any clinical risks.
If agreement can be reached with the patient then the practice should seek their consent to destroy the storage media concerned. If this is not possible, then the storage medium should be given to the patient for their own use. If this offer is declined, but the patient does not wish the storage media to be destroyed, then the practice should refer to the ICO in Scotland for advice, perhaps via their defence organisation. At this stage although the media item exists it does not contain any usable data, and as such no longer constitutes personal data (as it is corrupt or unreadable) and thus could reasonably be destroyed even without the patient's permission if the practice are unable to continue to store it indefinitely. Nevertheless, each case is likely to be exceptional so legal advice should be sought.
We would consider the more common scenario to be that the patient consents to the destruction of the media and assists the practice in identifying any significant history that may have been lost from the record.

2 Good Practice Guide texts:

CD-ROM based attachment transfer

Although GP2GP rollout continues to progress in England (and is the professionally preferred method of electronic record exchange) it is not yet available for all GP systems. As an interim step, an alternative means of transferring attached documents via CD-ROM disc has been developed by an IM&T Committee consisting of members of the Beds and Herts. Local Medical Committee, GPs, practice staff and PCT staff, working in cooperation with several GP system suppliers.

Detailed guidance on operating this CD-based transfer, including advice from individual GP system suppliers, is available from the project website[1].

The protocol has been operating successfully in a number of PCTs, to the benefit of both sending and receiving practices but the following principles and caveats should be noted;

- Formal permission should be sought from the Sending practice's PCO to allow CD-based transfer.
- The process should not be carried out until administrative staff have received training in the necessary procedures, as documented at the project website, both to create the outgoing CD and to import attachments from the received CD.
- The procedures advised by the appropriate GP system supplier should be closely followed to prevent potential loss of information in the transfer process.
- The recipient practice retains the right to receive the record and attachments in paper format if they so desire, but must request this from the sending practice in a timely fashion.
- Only non-rewriteable CD-based transfers are acceptable. Other media such as DVD, floppy discs and USB memory sticks have significant risks and drawbacks in comparison.
- After importing and checking the data, the CD received must be shredded or destroyed by cutting – the project website gives further instructions.

10.6.2.1.3 CD encryption issues

Department of Health information governance guidance suggests that where clinical documents are electronically transferred outside the practice, patient privacy should be protected by the use of encryption and passwords, in case of inadvertent loss or interception of the document in transit.

> *"David Nicholson, NHS Chief Executive, has directed that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is also now a requirement across all public sector organisations set by the Cabinet Secretary.*
>
> *It is recognised however that this may take some time to achieve in the NHS where patient care is our highest priority. NHS bodies will need to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether use of unencrypted devices should continue as an interim measure. Where it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the organisation's Board, so that the Board is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security."*[2]

This is one rationale for the use of approved NHS mail and messaging facilities such as the Spine and SCI-Gateway, which provide such security automatically for emailed attachments and clinical messages such as electronic referrals and GP2GP record transfers.

[1] http://www.starpace.co.uk/page.asp?pageID=97

[2] http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security/encryptionguide.pdf

To comply fully with the DH directive, a CD used for attached document transfer should be encrypted, but this considerably complicates the transfer process, requiring agreement on the encryption method, availability of the appropriate encryption/decryption software in both practices and communication of the associated password in a secure and timely fashion. If not handled correctly, it may also interfere with patient rights to access records under the Data Protection Act.

In view of such added complexity, the Beds and Herts. CD transfer project team judged that within this very specific context, encryption adds little to patient privacy protection, given that the CD-ROM is physically transferred via a secure courier service alongside a set of unencrypted paper printouts of other aspects of the clinical record.

Whilst generally acceptable to participating practices, PCOs and suppliers, this advice has not been formally endorsed by practitioner representative bodies, NHS, or medical defence advisers. It remains likely that in due course formal guidance will be introduced, jointly with the Department of Health, on standard methods of encryption of CD-based document transfers and associated operating procedures.

Until such time, where encryption is not used, practices should make an individual assessment of the risk of a privacy breach and agree the approach with their PCO.
Full Department of Health Information Security Guidance may be found on their website[3]

10.6.2.2 NHS Scotland

10.6.2.2.1 Docman Transfer
Almost all Scottish GP practices now use the 'Docman' document management package and associated standardised folder structure. The NHS Scotland Practitioner Services 'Docman Transfer' facility allows the automated transfer of attached documents between practices without the need for the documents to be re-filed in the recipient practice. In addition, an export of the entire GP system patient record to an electronic document may be made, imported to Docman and transferred electronically with the other attachments.

At publication, the 'Docman Transfer' facility was available to 95% of Scottish practices and for these practices represents the simplest and safest approach to attached document transfer. Details of the 'Docman Transfer' process are available online[4]

10.6.2.2.2 CD-ROM based attachment transfer
The use of compact discs (CDs) to exchange attachments or other electronic records is not currently formally supported by the NHS in Scotland. Any such arrangement would be strongly discouraged where 'Docman Transfer' is available but if necessary it should be agreed on a per-case basis between sending and receiving practices. The protocol used within NHS England for CD-ROM attachment transfer (see above) may be regarded as a robust model on which to base any local arrangement.

++++++++++++++++++++++++++++++

Data transmission - the practice has a responsibility to ensure that all data extracted from the patents' records are processed securely5. This includes making sure that the data leaves the practice securely. If it is to be carried on removable media such as USB memory devices or CD-ROMs, the data must be encrypted (and the key sent separately). If it is to be transmitted electronically, such transmissions must be secure. Once the data leaves the practice, the recipient may take over the responsibility of data controller for the data they hold, depending upon their use of the data.

[3] http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_074141.pdf
[4] http://www.psd.scot.nhs.uk/professionals/medical/DocmanTransfer.html
5 Legal Guidance on the Data Protection Act (1998), Information Commissioner's Office
http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf