BMA

# Principles for sharing and accessing local shared electronic patient records for direct patient care

British Medical Association
bma.org.uk

# Principles for sharing and accessing local shared electronic patient records for direct patient care

Until relatively recently, data recorded in GP systems have not been directly accessible by other organisations. Data have previously been shared via specific clinical communications, for example, by sending a referral letter. A number of system suppliers have developed systems which allow healthcare professionals from different organisations to directly access the detailed GP record.

Some GP practices have also implemented shared record systems as part of collaborative working models. GP networks allow individual practices to take advantage of the opportunities offered by providing services "at scale". In some cases, a number of single practices have asked their GP system supplier to treat them as a single entity with regard to their patient data, in order to increase efficiency in working. This has created a merged database of patient records[1].

The following principles are intended to support GP practices that are considering implementing shared record systems[2]. They are high level principles, which the BMA believes represent best practice in terms of allowing records to be shared in order to facilitate patient care, whilst maintaining high standards of confidentiality[3]. All system suppliers should aspire to meet these standards. Where practices work collaboratively but remain separate legal entities (and are thus still individually registered as data controllers with the Information Commissioner's Office), then the same principles apply to sharing as they would to sharing between separate organisations.

## Making patients aware of new arrangements

**1.** Patients must be made aware, in advance, of the new arrangements for managing their health information. This may involve a discussion with the patient during a consultation, an information leaflet being sent to patients and being made available in the practice or other forms of communication with the public. Communications should include posters in the practice, information on the practice website, or use of local media to raise awareness. Practices may wish to consult with their Patient Participation Group. Doctors should have confidence that these methods of communication have been effective.

Different suppliers of shared records stream/store data in different ways. For GP practices using EMIS Web and SystmOne, for example, patient records are held in a data centre. Patients cannot opt out of having their data held in the data centre; if a practice agrees to stream data this applies to all records. Having patient records stored in the data centre does not automatically mean that other organisations can view them; by default organisations should only be able to see their own records even though they are held in the same data centre.

With Vision 360, a copy of the GP practice records are streamed to a database for sharing. The default is to stream patient records, however, individual patients can opt of their data being streamed by using Read Codes. If a patient opts out, their data is not streamed into Vision 360, but will continue to reside within the Vision dataset at the practice, which could be held on a server at the practice or hosted in a datacentre.

1 This has created issues for some practices where the suppliers are no longer able to separate data for individual practices, including for national reporting purposes such as the Quality and Outcomes Framework. The Health and Social Care Information Centre has written to the suppliers, urging them to work with these practices to deliver a solution that maintains the benefits of shared records, whilst allowing individual practice data to be extracted.

2 For further guidance on shared electronic patient records, see Chapter five of the Good Practice Guidelines for GP Electronic Patient Records version 4 (2011): https://www.gov.uk/government/publications/the-good-practice-guidelines-for-gp-electronic-patient-records-version-4-2011

3 There may be additional issues, beyond the scope of this guidance, which relate specifically to sharing the ability to edit the patient record

## Establishing the organisations involved in the sharing

**2.** As data controllers, GPs should make decisions about which organisations access their patient records. GP practices should consider which organisations in the local health community are providing care to their patients and whether information sharing would improve the delivery of care, and is necessary for direct care.

It is good practice to establish formal sharing agreements between the different organisations involved in sharing. Practices working collaboratively should consider establishing formal arrangements between each practice to ensure a clearly documented understanding of how merged records should be managed. The Department of Health (DH) guidance[4] on shared records explains that participating organisations will become data controllers in common under the Data Protection Act 1998 for the information within the shared environment. We recommend that practices complete the checklist within the DH guidance of key issues for inclusion in local agreements.

With SystmOne, this involves accepting or rejecting a 'share request' for a particular patient from another organisation, such as the local care home. With EMISweb and Vision 360 this involves establishing a local sharing agreement with the organisation, which specifies the type of information to be shared e.g. demographics, consultations, medication and the job roles which can view the shared data.

## Options for restricting sharing and tailoring information

**3.** If patients are concerned about shared records systems then options for restricting sharing should be explained:

- Patients must be able to apply a blanket dissent i.e. I do not want my record to be shared with other organisations.
- If patients decide to have a shared record they should be able to make decisions about which organisations can access their records.
- If patients decide to have a shared record, their explicit consent to view must be obtained e.g. where a practice other than the patient's registered practice is seeking to view the record for the delivery of out of hours care.
- Patients must be able to mark specific items as sensitive/private which means they will not be visible in another care setting. Ideally systems should include the flexibility to allow patients to withhold particular items from specific organisations.

At present, the various systems provide the ability to withhold sensitive items in different ways. With some systems, if a patient withholds a sensitive item they withhold it from all organisations but with other systems there is greater granularity around who and which organisations can access the sensitive items.

**4.** In exceptional circumstances, for example if the patient is unconscious and immediate access to the record is necessary, it may be appropriate to access the record without consent to view. Healthcare professionals must indicate on the system a reason for this. An override may not be possible if a patient has dissented from a shared record.

As well as opting in or out from streaming as described in the first box, if a patient agrees to a shared record with Vision 360, they can specify which organisations can view their record by giving their consent to view at the point of care. Only the information that is set out in the sharing agreements, described in the second box, is shared; an OOH GP may have access to more enriched information from the GP record compared to a diabetes nurse. If the patient opts out of streaming then their record is not available.

With EMISweb, the patient has two options: either to share or not to share across organisational boundaries. If at this point they dissent, their information is not accessible by other organisations. If a patient selects the 'share' option then they can tailor which organisation can see their records by giving or withholding their consent

4 Department of Health guidance on shared records and data controller responsibilities https://www.igt.hscic.gov.uk/WhatsNewDocuments/NCRS.InfoSharing.Checklist.doc

to view at the point of care or by applying a confidentiality policy[5]. In addition, as with Vision 360, the information available is set out in the sharing agreement and tailored to the particular healthcare professional.

A share in/share out model is used for SystmOne. Taking the example of a patient being cared for by a GP practice, a community nurse and health visitor, at the first appointment with the community nurse the patient will be asked for their consent for the community nurse to view information recorded in other healthcare settings i.e. the GP record and the health visitor record. This is called 'share in'.

The community nurse will also ask the patient whether they are happy for the community nurse record to be shared with other organisations; this is called 'share out'. Patients must understand that it is the whole record from that care setting which will be visible if they give their explicit consent to 'share out'. If the patient dissents, the community nurse record will not be made available to any other organisation unless the patient changes their mind. Similarly, if the patient had dissented to a 'share out' at the GP practice, the GP record would not be listed for the community nurse to access it.

**5.** Healthcare professionals should only view the information relevant to their care setting, unless the patient has given their explicit consent for the full record to be viewed. In the BMA's view, it is unnecessary for a physiotherapist treating ligament damage to access the entire medical history, for example. Traditional referrals result in relevant information being shared with the treating clinician. This exchange occurs under implied consent. Systems that disclose the entire patient record to the treating clinician require explicit consent[6].

## Legitimate Relationships

**6.** Healthcare teams should only be able to view the records of patients with whom they have a direct clinical relationship. This means that the patient must be registered on the system of the organisation which wishes to view their record, for example as a result of referral. It should not be possible for one organisation to view *all* of the records of another organisation. It would be inappropriate for *all* patient records from a GP practice to be accessible at a local hospital because many of these patients will not be receiving care at the hospital so there will be no legitimate relationship. It is appropriate for GPs to view information recorded by other healthcare professionals when caring for their patients, unless the patient dissents. There may, however, be exceptions for example, some sexual health information[7]. Appropriate role based access controls should be in place to control access to patient data.

## Audit Trail

**7.** Systems must be designed to include audit trails. Ideally, these should allow patients to view details of who has accessed and edited their records and when. If a record is accessed without the consent of the patient there must be a mechanism to notify a trusted third party such as a privacy officer. GP practices should ensure that audit logs are reviewed so that any inappropriate access can be identified and acted on.

5 If a confidentiality policy is applied, to an individual item or entire record, access can be restricted. For example if a GP marked the whole GP record as 'doctor only' only the GPs in the GP practice could see the record. Records from the other organisations would continue to be shared in the same way.
6 In relation to TPP see box under point 4 with regards to sharing in and out.
7 In these care settings the patient in discussion with the healthcare professional should decide whether information can be shared with the GP practice.