Consent Model

It is recognised that there are concerns regarding governance, and patient confidentiality in particular, and this aspect of the PRN is taken very seriously by both GP Care and EMIS.

There is also a recognition, however, that, in order for clinicians to be fully informed when attending to a patient, there must necessarily be some form of data sharing. Governance is therefore focused on ensuring that the sharing of data is carefully monitored and controlled rather than prevented.

The PRN conforms to a Consent Model identified by Professor Trisha Greenhalgh in her evaluation of Connecting for Health’s Summary Care Record. It covers situations of both implicit and explicit patient consent. This consent model, which applies to the GP Care PRN, is fully compliant with the relevant sections of The Data Protection Act 1998, pertaining to the processing of personal data.

Dame Deidre Hine, chairman of the BMA’s working party on IT, said: “We support the recommendation to move to a ‘consent to view’ system which would meet much of the concern about informed consent expressed by doctors and gives patients appropriate control of their personal data.”

Deemed Consent
Where a patient is referred by the GP to a local NHS care provider, the patient is deemed to have implicitly consented for the provider to view the areas of their record, as set out in the Sharing Agreement between the practice and that organisation, for the specific episode of care.

Consent to View
In the situation where prior consent is not obtained, or is not implicit through the patient’s agreement to be referred to a specific individual or organisation, the ‘consent to view’ model will apply. This means users in organisations providing episodic care (such as A&E, OOH, etc.) are prompted to confirm patient consent to view the shared record when they access a patient’s care record, as no prior legitimate relationship is established as a result of referral.

The PRN meets these requirements and gives the patient ultimate control of their personal data. The PRN does, however, allow this consent to be over-ruled in the circumstances where the patient is unable to give consent, such as where patient consciousness is significantly impaired. Where consent to view access takes place, or consent to view is over-ridden, an electronic notification is made to the practice alerting their Data Controller to this data access, thus enabling verification that the access was legitimate.

GP Care and EMIS have taken all necessary precautions to ensure that the procedures proposed for accessing personal data comply fully with the Principles set out in Schedule 1 of the Data Protection Act 1998.
Frequently Asked Questions

Q. Who can access patient records on EMIS Web?
A. The registered GP Surgery controls access to their own patients’ records. Data is made available to approved, local NHS organisations via Data Sharing Agreements between the practice and the 3rd party organisation. EMIS does not, and will not, give access to patient records to any organisation other than those approved by the practice.

Q. What if one (or more) of my patients does not want their information streamed and stored in EMIS Web?
A. Every patient has the right to opt out of sharing their medical record. They can do this by completing an Opt Out request form. This is then logged within the EMIS Web system to prevent any part of their medical record from being shared. The GP should inform patients of the implications of ‘opting out’ and that any shared data would only be seen by healthcare practitioners who are treating or due to treat the specific individual, and only the areas of the record that the consulting doctor deemed relevant would be viewed.

If the GP feels that it would be detrimental to exclude the individual’s data from any sharing agreements, the data controller at the practice should then make a written response to the patient, explaining the reasons why they believe the patient’s request is not sufficiently justified.

Q. If a patient opts out, will GP Care still have access to information without patient identifiers?
A. No. If a patient opts out, no part of their medical record will be available to any 3rd party.

Q. How can I be sure no-one is accessing the data without consent?
A. No unauthorised bodies will ever have access to this data. The only way an individual can view a patient record is via individual log-on through a terminal with an EMIS Web application at an organisation which holds a Sharing Agreement with the patient’s registered practice. Any and every type of access is tracked in the audit trail, and the individual will only be able to access the areas specifically permitted in the Sharing Agreement.

Q. Will GP Care be able to see any named patient data?
A. Only if the Sharing Agreement states that GP Care can see patients’ names. For clarity, GP Care does not need or wish to have access to named patient data.

Q. Where is the data stored?
A. Data is stored in twin EMIS data centres. These centres are fully accredited to the ISO 27001 information security standard, and all EMIS data storage and management procedures and processes adhere to the rigorous ISO 27001 standards.

Q. Who ‘looks after’ the data stored in EMIS Web?
A. There is a separate database within EMIS Web for data from each PCT. These are only accessible by a Fully Managed Service (FMS) team, who have 24 hour access to the data centre. These data controllers have undergone rigorous background checks and have signed the necessary Data Confidentiality Policies. Any breach of confidence would be dealt with by the police and the relevant PCT’s.

If, for any reason, certain software is not functioning as it should, the FMS team can access the practice server remotely, or in person, to rectify the situation.
Q. **What if someone hacks into the central EMIS Web database?**

A. Any unauthorised access would only be possible from an EMIS module and via a secure N3 connection, i.e. by NHS Staff. Even then, there is an extremely high level of encryption applied to any data sent or stored in EMIS Web which, essentially, makes any attempt to gain access impossible.

Q. **What if we want to end the Sharing Agreement with GP Care and rescind the access that other organisations have to our patient records?**

A. Each practice has the right to deactivate a Sharing Agreement at any time. However, this decision should not be taken lightly and the practice should remind themselves of the benefits that EMIS Web provides before deactivating an agreement. The practice should also inform EMIS and any associated parties which hold Sharing Agreements, before taking such action.

Q. **What is GP Care’s role in this?**

A. GP Care manages the relationships between the practice and third parties with whom the practice wishes to share data. This involves specifying and agreeing the data content to be shared, drawing up the data sharing agreements and making data sharing arrangements available to the practice. The practice Data Controller then chooses to agree the specific data sharing agreement and switch on the data sharing process within EMIS Web.

Q. **Are all data sharing arrangements the same?**

A. No. The type of data made available is limited to the data sets that are required for a specific clinical purpose. There are broadly speaking two types of record sharing:

1. Caseload Sharing, such as when a referral is made to a specific clinic, e.g. Urology; or individual, e.g. District Nurse, where only specific, named patient records are made available to the approved third party.

2. Access to whole aggregated database, e.g. OOH or A&E, where it is not known in advance which patient will present. In this case, the approved third party is required to complete an on screen form recording that they have the patient's consent to proceed before they are able to open the record. The data shared will be either for a subset of the patient record or for the whole record as previously specified in the Sharing Agreement with the approved third party. This record access creates an automatic notification back to the practice that their patient’s record has been accessed.

Q. **Is there an audit trail?**

A. Yes, the comprehensive audit trail tracks every record access and all changes made to the patient's record. This includes who accessed it, which areas were accessed and when.

Q. **Does this put our patient information on the NHS Spine or create a national record?**

A. No. The spine is used to ensure secure transit of information, but the data remains under practice control on servers owned and managed by EMIS.

Q. **What should I tell my patients?**

A. It is good practice to inform patients when their records are being shared even when consent is deemed implicit in the decision to refer the patient. It is recommended that practices should publicise (perhaps via practice leaflets/posters in the waiting room and on their website) to their patients the circumstances in which their records will be shared and the patients’ right not to have their information shared.
EMIS Guidance

EMIS has provided further comments on confidentiality, integrity and accessibility, which are set out below:

Confidentiality
- Data is transmitted across the NHS N3 network and is encrypted (scrambled) in transit;
- Data is stored in the EMIS data centres. These centres are fully accredited to the ISO 27001 information security standard, and all EMIS data storage and management procedures and processes adhere to the rigorous ISO 27001 standards;
- EMIS will not grant anyone access to patient records. The GP practice controls access to records;
- All viewing of the record is recorded in the system audit trail;
- By default, only users in the organisation that own a record can view that record;
- Subject to mutual agreement, organisations can share records with each other when providing care for the same patient;
- Organisations can use confidentiality policies to restrict the viewing of and access to a patient record, or to individual items within a record;
- No organisation (for example, PCTs) can run a search on patient records unless an active sharing agreement is in place. It is anticipated that GP Care would facilitate anonymised data searches for PCTs.

Integrity
- The same information is stored both on EMIS LV or EMIS PCS and on EMIS Web, so there is no loss of information when using both systems;
- EMIS has established rigorous quality assurance procedures to ensure that data stored on EMIS Web is identical to that stored on EMIS LV and EMIS PCS;
- All coded clinical data is stored in both the current format of Read codes (Version 2)/EMIS drug codes and the equivalent identifiers of SNOMED CT/dm+d format within EMIS Web;
- Advanced messaging technology ensures that patient records both on EMIS LV or EMIS PCS and on EMIS Web are kept synchronised;
- If either EMIS Web or the local system fails, then the other system is still available. When the failed system is restored, the messaging technology ensures that the restored system is subsequently synchronised;
- Malicious access to the EMIS Web server farm is prevented by firewalls, which ensure that only the organisation that owns the record can access the data;
- EMIS Web servers are connected to the NHS N3 network, not to the Internet;
- EMIS data centres use the highest industry-standard storage area network (SAN) configuration. The SAN is a large series of hard disks that copies all data to a second SAN at a separate location. When data is filed at the first location, a copy of that data is written to both data centre locations, so that if there is a problem at the first location, the data at the second location is still safe. It is anticipated that the EMIS data centres will be accredited for IT DES component 4 payments and are comparable to Connecting for Health standards.

Availability
- EMIS Web servers have 99.99% availability. They are not shut down for nightly backup, and the system design means that if one server needs maintenance, another server takes over;
- EMIS Web is designed to ensure rapid loading of pages when the system is in use. EMIS is committed to making EMIS Web at least as fast and easy to use as EMIS LV and EMIS PCS;
- EMIS Web servers are accessible on N3 data centre links, which are resilient and mirrored at the secondary location. This means that if one link goes down, another takes over;
- The availability of the local or Enterprise (PCT wide) EMIS LV or EMIS PCS system means that if the N3 link to a practice is unavailable, the organisation still has access to patient records;
- To ensure business continuity, the EMIS data centres are at two physically separate hosting locations approximately ten miles apart, and operate from two different telephone exchanges.
This eliminates a single point of failure, for example, in the event of a system failure at one exchange;

- EMIS has its own mega-watt electricity substation and generator, which not only provides power to the main EMIS SAN location, but also enables EMIS to provide full services in the event of a local power failure. The substation also includes a backup generator which can power our main site in the event of longer term power failure;
- Secure EMIS hosting locations are equipped with full biometric security (for example, fingerprint recognition) to restrict access;
- A number of different technologies, selected as the best means to protect either the data or application availability, are used to maintain system continuity; not only is data protected by mirroring at a second location, but all application equipment is also duplicated.