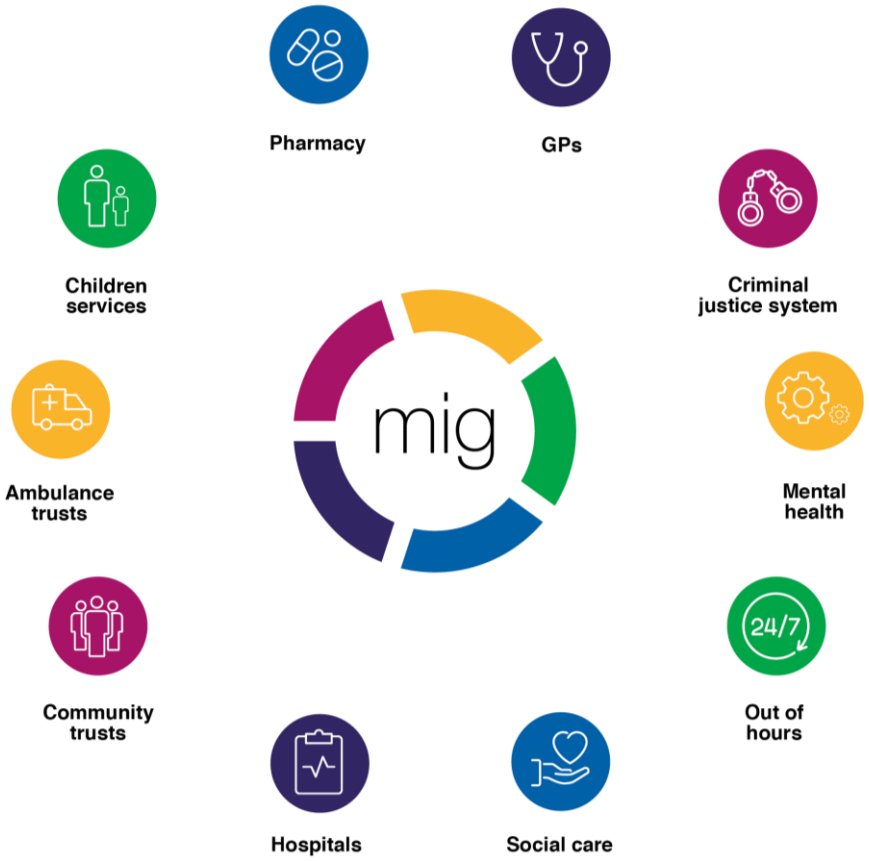
MIG Detailed Care Record data sharing and security

Overview

The Medical Interoperability Gateway (MIG) is a managed secure gateway to a set of services for exchanging real time data sharing between trusted and secure third party systems, meeting NHS Health and Social Care Information Centre Interoperability Toolkit interoperability standards. The MIG technology provides a secure mediation and brokering mechanism between trusted data providers and consumers, residing within the N3 network. Based on Enterprise Service Bus architecture, the routing of messages is entirely data driven, allowing the number of MIG services offered to grow without changes to core MIG functionality



The MIG connects and brokers' data through enterprise instances of data provider systems, therefore for those systems where data resides locally, for example on a GP surgery server, this data must be streamed in real time to the hosted environments before MIG enablement may commence.

- Security.
- Data is transmitted across the NHS N3 network and is encrypted (scrambled) in transit.
- The MIG web service uses transport level security (TLS) to secure connections and synchronises its clocks using an N3 time synchronisation service. MIG uses X.509 certificates to authenticate client systems and create Digital Signatures (based on XMLDSig Specifications) which are used to mitigate against replay attacks.
- The MIG is compliant with the following web standards based on the ITK guidelines:
    - WS-Security.
    - WS-Addressing.
    - XMLDSig.

MIG Detailed Care Record service

The MIG Detailed Care Record service caters for the real time retrieval and display of GP held patient record detailed information. The service provides fully embedded, integrated access to primary care patient records from trusted third party applications. Subject to appropriate enabled sharing agreements, data is presented as a common HTML read only view. Information is displayed in ten views based on a fixed content model consisting of all or a subset of the following:

1. Summary.
2. Problems.
3. Diagnosis.
4. Medication.
5. Risk and warnings.
6. Procedures.
7. Investigations.
8. Examinations (BPs only).
9. Events (encounters, referrals and admissions).
10. Demographics.

All sharing organisations must agree to share the same views with an individual viewing organisation.

Sharing agreements

Prior to the technical activation of the MIG Detailed Care Record service in any given locality, Healthcare Gateway requires written evidence from the data controller they agree to share their data by way of signed data sharing agreements

This agreement must cover the provision of data by a number of organisations (the sharers/provider) and access to that data or views on that data by a number of organisations (the viewers/consumer).

- Sharing agreements are set up between the share/provider and viewer/consumer organisation for example between GP practices and the local out of hours provider.
- Access to the data from the MIG is based on the sharing agreement and only the agreed data set is shared.
- The MIG holds a summary of the sharing agreements consisting of the fact of the agreement and the identities of the provider and consuming organisations.
- All sharing organisations must agree to share the same level of data with an individual requesting organisation.
- The requesting application, e.g. the out of hours' system, will be configured to only access practices who have agreed to share data with the OOH service.

Consent and permission to view

Data providers

Healthcare Gateway are mandated by the consent model as dictated by the system in use by the sharer/provider organisation in terms of consent to share (i.e. implied or explicit consent). It is the responsibility of the sharer/provider system to only provide data for patients that have the correct consent setting.

Data consumers

Healthcare Gateway are mandated by the consent model as dictated by the system in use by the viewer/consumer organisation in terms of consent to view. It is the responsibility of the system that is consuming the MIG service to request permission to view or to bypass the permission if the consent setting is appropriate and store and audit the permissions.

For further information on how sharing and consent is managed by consumer or provider systems, please contact your software supplier.

User role based access control

Systems that consume MIG services should support the concept of user roles that enable some users to view shared data and restrict others without the appropriate access rights.

For example it may be determined that certain administrative staff should not be provided with data from sharer records and limited to the data within their own organisation's records. Wherever possible, role profiles should be aligned with the NHS RBAC definitions. It is the responsibility of the viewer system to manage role based access. Neither the MIG, nor the sharer's system take part in the validation of user's rights to access.

For further information on how role based access is managed by consumer systems, you should contact the your software supplier**.**

Legitimate relationship

Systems that consume should support the concept of a legitimate relationship, which is a means of determining and auditing whether a particular organisation is providing care for the patient and that the patient has given consent for their record to be viewed via the MIG. For example, it should be audited that the patient has given consent before patient data is requested. If the patient is not able to give consent, due to an emergency situation or they are otherwise incapacitated, this should also be logged along with the reason why consent was not able to be obtained.

Legitimate relationship support should be aligned with NHS requirements

For further information on how the legitimate relationship is managed by consumer systems, you should contact your software supplier.

Audit

To enable the sharer/provider organisations to audit access to patient records, systems that view/consume MIG DCR services must include information to identify who and when an extract was made in the MIG extract message

It is the responsibility of the sharer/provider system to audit the information provided in the MIG extract request when patient information has been accessed by an external organisation.

For further information on how audit is managed by consumer or provider systems, you should contact your software supplier**.**

Disclaimer

Associated documentation

- HGQM009 Healthcare Gateway MIG Content Model Read Code Mappings to Record Elements.
- EXT584 TPP Implementation of the MIG DCRV1 Content Model.

Contact information

Healthcare Gateway, Fulford Grange, Micklefield Lane, Rawdon, Leeds, LS19 6BA.
enquiries@healthcaregateway.co.uk
www.healthcaregateway.co.uk
0845 601 2642