BMA

Focus on GP Data Sharing and GP data controllership

Summary

GP contract holders determine the purposes for processing their patients' personal data and the means of processing the data. Under data protection law GPs are the 'data controller' which means they are effectively the legal guardian of all patient data in the GP medical record. (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/)
Patient data can be accessed by the patient (the 'data subject'), or other health and social care providers involved in a patient's direct care. Patient data held within GP IT systems has the software supplier themselves acting as the 'data processor', a position that makes the system supplier accountable to act on the instructions of the data controller, the GP contract holder(s).

It is the trust enshrined between GPs and their registered patients which underpins the confidentiality of the patient's GP record. Recent times have seen Government repeatedly seek to impose measures that would potentially damage this relationship – be that the adoption of GP Data for Planning and Research (GPDPR) that seeks the lifting of GP data wholesale, to be shared at the discretion of the Department of Health and Social Care for reasons beyond direct care, or efforts by Government to bypass GPs and instruct software suppliers to flow patient data directly onto the NHS App platform, despite any potential risks such action may pose.

Patients have the utmost trust in their GP and believe anything they tell them in the confines of the consulting room will remain confidential and only be used to enhance the care they receive or for bona fide clinical research. Any undermining of this trust, with data being used for other reasons, has the potential to seriously affect the patient/doctor relationship.

The future of the GP Record

Despite repeated attempts to undermine GPs' control of the data of patients under their registered care, there is no way to force a GP to relinquish data controllership, unless the Government changes the law to remove or amend their controllership
Despite this, there have been indications that Government is exploring using to transfer patient data out of the general practice record.

GP Connect, sometimes referred to as an NHS Direct Care Application Programming Interface (API) tool, is an NHS IT service which allows GPs as data controllers to share a view of the electronic GP patient record with authorised and audited healthcare staff (e.g. out of hours services and emergency departments). Programmed on NHS smartcards, clinical systems use role-based access control (RBAC) for the purposes of direct care, to share and view GP practice clinical information and data between IT systems quickly and efficiently in real time, so they can see relevant coded history, medications, allergies and appointment

information. **GPC England wholeheartedly and unequivocally supports the use of data sharing for direct patient care.** Within England, an ICB may operate a local data platform, which may be able to use GP Connect to ingest, as data controller systems into a federated model to align with the ambitions of the Federated Data Platform. It is important to note that this functionality exists and has been recognised by NHSE. GPs as data controllers need to be aware of associated risks potentially posed by such a model.

GP Connect
https://digital.nhs.uk/services/gp-connect/gp-connect-in-your-organisation
The BMA's GPC England team would also bring to GPs attention another function within GP Connect:

Adding data into the GP Clinical Record
GP Connect has additional functionality whereby any permitted third-party provider may be permitted to not only view the GP clinical record, ***but also add data directly into it***. Such a function could potentially further enable workload transfer from an external provider directly to the GP in the future. An example may be an approved private psychiatry provider diagnosing ADHD in a patient being seen remotely, adding a code to the patient record, and initiating medication with the expectation for the GP to continue to manage, monitor and prescribe. Such a process may not give thought to the workload or capacity impact upon the GP or practice.

The national data sharing arrangement allows any party the ability to withdraw consent to have data added to the patient record at any point for any reason. **There is nothing presently within the GMS contract which mandates the acceptance of GP Connect Update Record functionality. Practices struggling with workload and capacity may be advised to switch off the functionality of adding data to the GP patient record, to support the BMA's safe working guidance.**

If a data controller was wishing to suspend the ability for an external provider to directly add information into the patient record, then they can do this by disabling the service. Instructions are below for the two most used clinical systems.

EMIS
To amend the GP Connect Update Record functionality, in Organisation Configuration, select Edit Organisation, then scroll down to the option Accept GP Connect Update Record via MESH and select Yes. Click OK to save. You will be prompted to restart EMIS Web to complete the activation.

This is a screenshot of how that page looks
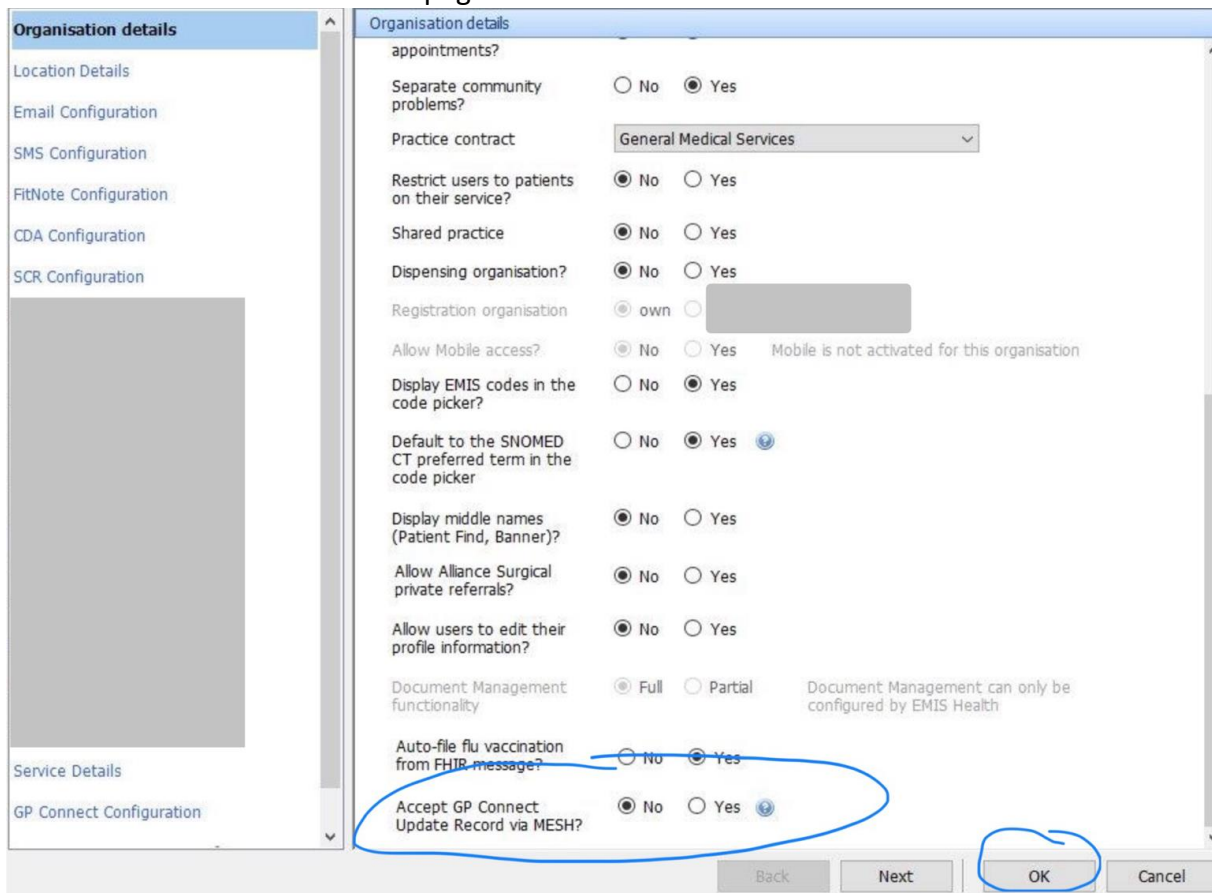
TPP

In Organisation Preferences the screen below explains how you can click different options to provide different access to your system. Clicking 'off' means no incoming data will be automatically filed into your system.