**GP Practices (Update)**

**Update: we have updated the guidance in the last paragraph based on feedback from the Joint GP IT Committee.**

Dear Customer,

As you may be aware, recently, the Secretary of State for Health and Social Care published his technology vision, “The Future of Healthcare”[1], which includes as one of its fundamental principles the concept of ‘Internet first’. In response to this driver there is a requirement in IT Futures, the framework which will be replacing GPSoC, for all systems vendors to adopt a cloud computing policy by July 2021.

In parallel, EMIS has recently announced its future upgrade programme for EMIS Web to create a more modern, cloud based system with improved interoperability capabilities. We expect this to be a cornerstone that supports GPs and CCGs, facilitating integrated working (including Primary Care Networks) across primary, community, acute and social care. This will not be a ‘big bang’ change; rather it will be a progressive transition over the next few years so as not to disrupt your day to day working.

EMIS and the EMIS National User Group (NUG) have been working together to ensure all aspects of the EMIS transition strategy are understood and addressed. One key component of this strategy is to remove the reliance on EMIS’ existing hosted data centres and migrate (again, progressively and safely) to a state of the art cloud environment. EMIS has been working closely with NHS Digital to ensure clinical safety and Information Governance sign off, as well as contractual approvals, are all in place.

EMIS’ ongoing commitment to business continuity, and to providing the highest level of service to our customers, means that we will be making changes to the way we store data in EMIS Web. With effect from 10th June 2019, EMIS will start storing your practice’s EMIS Web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services (“AWS”). The data will remain in the UK at all times and will be fully encrypted both in transit and at rest. In doing this, there will be no change to the control of access to your data and the hosted service provider will not have any access to the decryption keys. AWS is one of the world’s largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the very highest levels of security and support.

The first data we will be transferring are clinical documents and over time, other data will follow. Access to this information for interoperability and reporting does not change and all data remains under the control of the practice through the Data Sharing Module in EMIS Web. We do not envisage any impact on EMIS Web users’ experience, indeed we expect that many operations will actually become faster.

As always, we really appreciate any and all feedback in respect of our services. If you have any queries regarding this change (or any other aspect of the service) then please do not hesitate to contact us on future-data@emishealth.com and we will be happy to discuss this with you. To be clear, EMIS will still be supporting, updating and developing EMIS Web during any transition period.

We will share user feedback and any comments raised by our users with the NUG to ensure there is ongoing transparency around this process.

What do I need to do next?

In addition to sharing any comments or queries you might have with us, we recommend that you use this as an opportunity to review your practice’s Privacy Notice to ensure that Patients have all the relevant information that they require regarding (amongst other things) any recipients of their data.

The guidance provided by the ICO refers to controller’s providing details of “the recipients or categories of recipients of the personal data”. Set out below (by way of information only) is some example wording regarding service providers such as ourselves which may be of assistance in revising your own notices (though clearly it would need to be tailored to reflect your own particular circumstances):

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties includes:

• Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.

• Delivery services (for example if we were to arrange for delivery of any medicines to you).

• Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third party processors can be supplied on request.

As a controller you should inform your Patients (e.g. via posters or general communications) and undertake a Data Privacy Impact Assessment (DPIA) in relation to this change. Further supporting information is available here. We hope that this information, together with this letter, will assist your DPIA considerations and if you require any further detail then please do not hesitate to contact us and we would be happy to assist.

The safety and availability of your data is our utmost concern and we are confident that this approach will improve data security, integrity and performance.

Best wishes,

Shaun & Vanessa

Dr Shaun O’Hanlon

EMIS

Vanessa Young

EMIS National User Group