DPO Newsletter 10/07/2018

Subject access requests, GDPR compliance checklists and practice DPO visits

Subject Access Requests

We have completed the first 11 practice DPO visits in order to determine what practices need from the DPO and what the DPO needs to do for the practices. Thank you for the very kind hospitality that we have received from practices and for the many useful ideas and tips that we have been given.

The most pressing GDPR issue has been Subject Access requests (SARs) and there have been many different stories and experiences shared.

The requirements for insurance reports and solicitors reports are slightly different and I have attached a Lanarkshire paper on the role of the GDPR and the Access to Medical Records act (AMRA) which seems to clarify the issues well. This paper also states quite confidently that practices cannot charge for postage of SARs.

There are three other papers about SARs attached: the first is a series of emails between Dr Paul Cundy and other doctors outlining the GDPR purpose of SARs being for checking that the data is being processed fairly and not for other purposes. This point may not gain support from the ICO.

The second piece of correspondence is kindly shared By Dr John Danson and includes his letter to Elizabeth Denham, the ICO, about the time and resources needed to respond to SARs and the reply to Dr Danson from Ms Denham's staff.

The third is a letter from a practice, outside of the West Pennine LMC, to an MP. The letter contains strong personal opinions but may be of use to practices who wish to pursue the issues of resources for SARs with authorities.

I am sorry that I can give no more specific advice at present and hope that practices, LMC and DPO can keep in regular contact to seek best practice for dealing with SARs.

Data Security and Protection toolkit is replacing the IT governance toolkit

- Training for practices

I would encourage you to book on to the training sessions for the new Data Security and Protection Toolkit, which is to replace the IT Governance toolkit. The two training webinars are available to GPs and practice staff on **24th July and 30th August** and can be booked via the following link:

https://www.dsptoolkit.nhs.uk/News/10R

GDPR compliance checklists and practice DPO visits

Practices have done a lot of work to read about and understand the GDPR requirements.

All practices have aarranged for someone to read the BMA, ICO and IGA guidance on GDPR.

Not all practices have identified DPO team members – the IT lead, Caldicott guardian, Practice manager, a partner, nurse etc and I would recommend that they do.

Practices are beginning to keep the DPO team member up to date with the BMA, ICO and IGA guidance when they have identified who the DPO team member/s is/are.

Practices do seem to be aware of their new data controller responsibilities

Not all practices have drawn up a plan to reach 100% compliance with GDPR within a reasonable date, for instance by 01 11 2018. However completing the actions in his checklist should help practices reach 100% compliance.

Some practices have arranged meetings with all of their partners, salaried doctors, nurses, PAMs, and all of their staff to set out the broad changes of GDPR. Some have not.

There is some uncertainty about ensuring that their CCG IT agreement is signed his and I suggest that practices that are unsure contact Sheila Mills at sheila.mills3@nhs.net

Quite a few practices are unsure about reviewing what data processing they undertake in the practice. I have attached two spreadsheets of data flow records that have been shared with us that may help.

Practices are not yet sure how to review what data processing is done on their behalf by external processors, and what data they use to do this.

“Check with your CCG what local data extractions your practice is involved I”. The CCG are compiling a list of local data extractions which I hope to share with practices soon. *

Most practices have created and publish any necessary Privacy Notices which are put on websites and on waiting room walls.

Nobody has created a data processing register and I have not yet ascertained what a data processing register is. For the time being I suggest that a data processing register is the record of data flows and data processing on behalf of the practice.

“Check with any other non NHS bodies such as researchers or institutions that you have a suitable contract and consent in place”. No practices so far have had researchers or other institutions processing their patients’ data.

Practices seem to understand about collecting consent for non-direct care communications with your patients. Sending invitations to invite practice patients with a long term condition to attend an education or health promotional event that will help the patients’ management their long term condition is fine. Inviting patients to volunteer to help another organization with voluntary work is for non direct care and requires explicit consent.

Every practice is struggling to manage and to revise their SAR handling arrangements to meet the new options and deadlines. CDs, encrypted CDs, patient access to records are being considered. Emailing encrypted bulk digital records has not worked for one practice as the files were too large. The attached Lanarkshire paper gives quite good advice on what is suitable to do when passing SARs to patients or their solicitors or insurers.

“Revise your data breach detection and reporting arrangements” Practices seem to understand how to do his and I have seen good Breach report forms on First Practice Manager.

“Set a program of GDPR training for your staff” This seems to be ongoing for practices.

Thank you for the invitations to visit practices.

Yours Sincerely,

Richard Fitton DPO