

West Pennine LMC Data Protection Officer Newsletter : June 2018

Queries

The DPO function has received over 10 queries from practices so far. The majority concern SARs (Subject Access Requests) made by solicitors or insurers but we have also had queries that concern Freedom of Information (FOI), inviting patients to public health promotion events and excluding third party data from SAR communications. We are creating a log of these queries and I will share anything that may be of interest to practices.

Breaches

We have been informed of three breaches, one of which had been (correctly) reported to the ICO using an ICO breach report template. It is important to note that breaches that need reporting to the ICO (see below) should be notified within 72 hours of their detection. **You do not need to report every breach to the ICO.** The ICO website has useful information on reporting breaches: <https://ico.org.uk/for-organisations/report-a-breach/>

“GDPR or DPA 2018 personal data breach: From 25 May 2018, if you experience a personal data breach you need to consider whether this poses a risk to people. You need to consider the likelihood and severity of any risk to people’s rights and freedoms, following the breach. When you’ve made this assessment, if it’s likely there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. **You do not need to report every breach to the ICO.**”

Preparing before and after DPO visits

The GDPR requires the DPO to have a close relationship with the organizations that he/she serves. We are arranging to visit to all LMC levy paying practices. We suggest that, before, and at the visits, practices address the issues that Dr Paul Cundy chairman of the BMA GPC IT committee Policy Lead suggests:

- Arrange for someone to read the BMA, ICO and IGA guidance on GDPR.
- Identify DPO team members – the IT lead, Caldicott guardian, Practice manager, a partner, nurse etc,
- Keep the DPO team member up to date with the BMA, ICO and IGA guidance.
 - **Get the DPO to assist you to**
- Ensure that the practice is aware of its new data controller responsibilities
- Draw up a plan to reach 100% compliance with GDPR within a reasonable date, for instance by 01 11 2018
- Arrange meetings with all of your partners, salaried doctors, nurses, PAMs, and all of your staff to set out the broad changes of GDPR.
- Ensure that your CCG IT agreement is signed
- Review what data processing you do in the practice
- Review what data processing is done on your behalf by external processors, and what data they use to do this
- Check with your CCG what local data extractions your practice is involved in*

- Create and publish any necessary Privacy Notices
- Create and have available your data processing register
- Check with any other non NHS bodies such as researchers or institutions that you have a suitable contract and consent in place
- Check that you are collecting consent for non-direct care communications with your patients
- Revise your SAR handling arrangements to meet the new options and deadlines
- Revise your data breach detection and reporting arrangements
- Set a program of GDPR training for your staff

*We have written to the DPO for Tameside and Glossop CCG (who is the DPO for Tameside Metropolitan Borough Council) requesting a list of all GP data flows to the CCG and will share it with all practices when we have received it. This list may help practices to create a list of their data flows.

SARs (subject Access requests)

We are grateful to Dr John Danson for allowing us to share the letter that he wrote to Elizabeth Denham, who is the current ICO. <https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf>

John is awaiting a reply and I think that his letter clearly states many of the issues that practices are concerned about.

We are also grateful to Stephen Healey Practice Manager & NHS Oldham Clinical Commissioning Group Board Member for allowing me to copy and share the email comments that follow Dr Danson's letter.

From Dr John Danson,

"Dear Elizabeth Denham,

My name is Dr Danson, a GP, from Oldham. I am writing regarding my concerns about the new rules following the Data Protection Act on May 25th. I am now receiving letters refusing to pay our fee requests from solicitors when acting as third parties for SAR requests for our patients. We usually charge £50 for copies of paper and computer records for stationary, administration staff time, postage and packaging and most expensively the GP time needed to check every part of the notes for third party references to ensure these are removed.

I understand the logic of free access as per the freedom of information act but with regards to medical notes it takes usually 30-60 minutes of GP time to properly check these notes. As an average size practice we usually do 3 sets of notes a week; we currently have to employ other clinical staff to free our GP time up to do this.

I understand a charge can be invoiced if the GP feels the request is manifestly unfounded or excessive, quoted as being a rare event but nonetheless apparently a subjective judgement by the GP practice. Our practice thinks any use of GP time in these administrative efforts should be deemed excessive when it is time that could be spent clinically face to face with sick patients.

Currently I have a solicitor's letter telling me charges should not be raised for this service and saying they will report the practice to the ICO if the notes are not sent by 13.7.18.

If I write back invoicing again saying the fee is still £50 for what we deem excessive and they report this to you could you let me know pre-emptively what you would do. Also can you voice the above concerns to the relevant bodies?

Many thanks for your time.

Dr John Danson »

Stephen Healey's email with a link to the BMA blog

From Stephen Healey:

"Hi,

The saga continues and it appears Paul Gundy's blog was updated yesterday with what looks like a "we cannot charge for copies of medical records" a link is below read it:

<http://www.pulsetoday.co.uk/your-practice/practice-topics/management/how-to-handle-subject-access-requests-under-the-new-data-regulations/20036599.article>

I think there may be more twists and turns in this before we finally get something definitive but my suggestion for the time being is not to ask for a charge for copies of records."

Kind regards,

Steve Heaney

Practice Manager & NHS Oldham Clinical Commissioning Group Board Member"

Information sharing agreements

Sheila Mills, who most of you in Tameside and Glossop will know as the GP IM and T Project manager for NHS Tameside and Glossop Clinical Commissioning Group, is responsible for managing the Information sharing agreements. She has three agreements in place or near finalization:

1. EPaCCS "Sharing Palliative and End of life Care Information. This agreement is between all Tameside and Glossop GP practices, Tameside and Glossop Integrated Care Foundation Trust (TGICFT), GoToDoc GP out of Hours, Willow Wood Hospice, North West Ambulance Services (NWAS) and The Christie.
2. Seven day access
3. Multidisciplinary team meetings access.

Sheila, and I will be meeting the Chief Information Officer and the DPO for Tameside and Glossop Integrated Care Foundation Trust (TGICFT) at TGH on July 10th to discuss the EPaCCS and I will cover all three agreements in future newsletters.

Finally: "Each General Practice must have a named partner, board member or equivalent senior employee to be responsible for data and security in the practice"

CCG Practice Agreement section 5.3 "Each General Practice must have a named partner, board member or equivalent senior employee to be responsible for data and security in the practice. This

requirement further defines existing practice obligations to identify the person with lead responsibility for IT in the practice.”