LMC DPO newsletter 3 from the West Pennine LMC DPO Office

Appointment of deputy DPO and DPO administrative assistant

Jane Hill, our LMC Liaison Officer, has been appointed as the deputy DPO and will understudy the DPO role for three hours a week from the 20th September.

Sue Gilks has been appointed as the administrative assistant to the DPO. Sue has a depth of experience of General Practice and of IT and can be contacted at westpenninedpo@btconnect.com. Sue will be working from the LMC administrative office for five hours a week on Thursdays Sue will be arranging visits, filing documents and correspondence, helping to define data flows and helping practices to maintain their IG (DSPToolkits) toolkit status.

Progress of the GDPR

Three months have gone by since the implementation of the European Union General Data Protection Regulation and of the 2018 Data Protection Act. The EU regulation covers 508 million inhabitants in 27 European countries — the world's third largest population after China and India.

The new regulation,which can be accessed neatly at https://gdpr-info.eu/, lays down "rules relating to the free movement of personal data"as well as rules relating to the protection of natural persons with regard to the processing of personal data". "The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data". I interpret this as an Act to improve but safeguard the benefits of the flow of European citizens' data.

Progress of the 2018 Data Protection Act

The Data Protection Act 2018 came into force on the same day as the GDPR. The Data Protection Act 1998 is a United Kingdom Act of Parliament designed to protect personal data stored on computers or in an organised paper filing system. It is a national law which complements the European Union's General Data Protection Regulation. Itupdates data protection laws in the UK. http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

The 2018 Data Protection Act makes provision for the processing of personal data most of which is subject to the GDPR.Part 1 of the Act outlines its purpose. Part 2 supplements the GDPR.Part 3 makes provision for law enforcement purposes. Part 4 makes provision for the processing of personal data by the intelligence services.Part 5 makes provision for the Information Commissioner.Part 6 makes provision for the enforcement of the data protection legislation.Part 7 makes supplementary provision.

Is the GDPR good or bad for General Practice?

GPs generally approve of measures that make them no less money, make their job no more difficult and make their job no less enjoyable. The GDPR seems to make GPs less money, takes up more of practices' time and reduces thetime for other General Practice tasks. However, a number of technologies and solutions seem to be coming to the fore that may reduce the workload of GDPR in relation to solicitors' and patients' requests and they are described below. There is also evidence that patients access to and use of their own records reduces consultations and phone calls from

patients to practices (1, 2) and that patients who are health literate and "activated" take up less NHS time and are healthier so needing less care. (3,4)

Confidentiality versus patient safety–to share or not to share – that is the question.The financial costs of data breaches versus costs of not sharing data

Principle 7 of Dame Fiona Caldicott's 2013 review states that "- The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies"

A report found that "the total sum set aside by the treasury for present and future claims for compensation related to clinical errors and omissions is £65,000,000,000 taking funding away the NHS and driving some GPs out of practice." "Non-medical aspects of patient care - cited as communication issues or staff attitudes - were a factor in almost half of all complaints investigated last year by the ombudsman Dame Julie Mellor. Poor communication, including quality and accuracy of information, was a factor in 35% of all complaints - though this was lower than the 42% in 2013-14". (5)

"The report found that the UK rivals the United States for compensation paid out, with Britain's medical-legal bill now £24 per person, more than twice the £9 per person in the US, despite the country's reputation for a more litigious culture."

Additionally, the MDU's costs for the year ending March 2016 were £1,400,000,000 and the bill is increasing by roughly 10 per cent each year.

On the other hand, the total amount of ICO fines on health service providers for breaches May 2016 to August 2018 (we have lost our pounds sign on the PC) was minute in comparison - #290,532. Most data breaches did not cause the physical harm that clinical errors caused, although some caused social and mental harm.The ratio of the financial costs of clinical errors to the financial costs of data breaches is 1000 to 1.

30% of clinical claims for compensation were caused by non clinical factors - mainly poor communication – so we could say that the ratio of financial costs from clinical to confidentiality errors was 330 to 1. The health costs ratio is probably higher taking into account that errors of clinical management generally might cause more harm than errors of confidentiality. It does not seem such an attractive option to share so little data in the NHS and Social Care sectors when so much harm comes from poor communication.

Managing insurance companies' requests for letters

Maureen H Falconer, Regional Manager – Scotland, Information Commissioner's Office, 45 Melville Street, Edinburgh EH3 7HL, recently wrote that "by 2015, it had become evident that insurers had changed established practice in favour of the SAR process under the data protection right of access. The ICO held talks at that time with the Association of British Insurers (ABI) to raise our concerns that a SAR was inappropriate when it should have been a request for a medical report. The ABI issued guidance instructing its members not to use the data protection legislation when it was a medical report they were seeking and that AMRA would be the legal gateway for disclosure rather

than data protection. Therefore, when an insurer makes a SAR as a proxy it will be prudent to clarify whether it is seeking full disclosure of the record or a medical reportso that the correct legal gateway may be used."

Managing solicitor's requests for letters

Here are a few tips shared by practices:

1. Speak or write to patients to ask them if they do actually wish to share the whole record with the solicitor or just the parts relating to their claim. It seems that a majority of patients have not understood the fact that the solicitor has requested everything that is in the record. Patients can clarify,for the practice, what they are happy to share with the solicitor. (The GDPR states that data that is processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
2. Although the law company, Manse, Pennington, advised against the practice, one practice is successfully and comfortably asking patients to pick up and sign for the SARs. It is working well. When some solicitors say that they do not want a patient to pick up the SAR in case they change it remove part of it that implies that the data request is not a SAR.
3. Ask solicitors to clarify the purposes for which they processing the patients' data and for which they require the data. As long as this request to the solicitor is made within a short interval from receiving the solicitor's request the 30 days required to process the SAR can be extended to stat from the date of the receipt of the answer from the solicitors.
4. Consider using iGPR, a system that produces ASRs automatically and removes third party data. Practices are examining the use of these systems and there has been a suggestion that the practices could bulk purchase the system as the cost is the same for every practice whatever the number of patients.
5. It is best for reasons of securityof processing of personal data to insist that the solicitor arranges to pick up the SAR from the practice. Secure a signature from the courier. (6)
6. Another practice is considering burning SARs onto a CD. CDs do not have to be encrypted when they are being collected and signed for by a patient, solicitor or his agent when their identity has been checked.
7. One practice is utilising their privacy notice to attach to copies of the patient records when giving the record to patients to comply with this requirement. The GDPR expects patients who make SARs to be told how their data is being processed as well as to see the data that is being processed. Attaching the privacy notice to the SAR seems to be a neat and simple time saving process.
8. Some practices are encouraging patients to sign up for complete record access. The patients can then use the @share@ button to share the record with the solicitor. (7)

SARS

Recent ICO Officer's response to a query from PM David Vincent, published in a PM's blog

Microsoft Word Document

Information sharing agreements

A majority of practices have signed up for the EPaCCs end of life sharing pathway. Templates for entry of data to the EPaCCs need to be agreed and practices may be able to allow the TGICFT to see the end of life wishes of their patients before the end of the year.

Tameside and Glossop Integrated Care Foundation DPO team

Breaches

We have been notified of 5 data breaches. One concerned more than one patient and the others concerned only one patient in each instance.

The breach of multiple data subjects was caused by using the CC instead of the bcc to copy in patients of a virtual PPG group. This inadvertently allowed the patients in the group to see each other's email addresses and indirectly their identity. This was a breach which had to be reported to the ICO. The ICO has replied and the case has been closed.

The other breaches were: putting the wrong letter in the wrong patient's envelope, pasting the wrong patient's details into a referral letter, putting the wrong patient's details on a certificate, a patient seeing another patient's information through record access for reasons of a technical nature and two patents in separate practices concerned that other patients could overhear their requests for prescription items at the reception desk.

To decide whether a breach has occurred and whether it needs to be reported to the ICO the ICO has produced his advice https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

In brief

"What is a personal data breach?

"A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

“Example

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

“A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

“Recital 87 of the GDPR makes clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

“What breaches do we need to notify the ICO about?

“When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it’s likely that there will be a risk then you must notify the ICO; if it’s unlikely then you don’t have to report it. However, if you decide you don’t need to report the breach, you need to be able to justify this decision, so you should document it.

“In assessing risk to rights and freedoms, it’s important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

“A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.”

“This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

Richard Fitton DPO West Pennine LMC

Jane Hill deputy DPO electWest Pennine LMC

Sue Gilks DPO administrative assistantWest Pennine LMC

1 “The impact of patient record access onappointments and telephone calls in twoEnglish general practices: a populationbasedstudy”, Caroline Fitton, Medical Student, Homenden hospital London, Richard Fitton, General Practitioner, Amir Hannan, General Practitioner, Brian Fisher, General Practitioner, Lewisham CCG, Lawrie Morgan, Economic Adviser, David Halsall, Principal Operational Research Analyst, Department of Health, London, UK

2 “Accessing personal medical records online: Ameans to what ends?*Syed Ghulam Sarwar Shaha, Richard Fitton, Amir Hannan, BrianFisher, Terry Young, Julie Barnett*,

3 Securing Good Health for the Whole Population 2004 Derek Wanless report to the prime minister, the secretary of state for health and the chancellor of the exchequer.**

4 Sondra Roberto 28 November 2012, Health Foundation article on patient engagement by Sondra Roberto 28 November 2012

5Parliamentary and health service ombudsman Complaints about acute trusts 2014-15

6 Article 5 GDPRprocessed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)

7 GDPR Article 2 “This Regulation does not apply to the processing of personal data:by a natural person in the course of a purely personal or household activity;”

** "We are not tinkers who merely patch and mend what is broken... we must be watchmen, guardians of the life and the health of our generation, so that stronger and more able generations may come after" Dr Elizabeth Blackwell (1821-1910), The First Woman Doctor