EQUiP

ENABLING QUALITY IMPROVEMENT IN PRACTICE

Tower Hamlets

# LATEST NEWS 30/04/2018

The first of many exciting things is that practices will effectively become data controllers. This means practices determine the purposes and means of the processing of personal data including patient data. I know what you're thinking – this is going to set the world of personal data ablaze as we can do whatever we want with it. This is partly true and partly not. It's true because we can technically do what we like with the data. It's not because there are a number of controls we need to put in place. The first is the appointment of a Data Protection Officer or DPO for short. The job of the DPO is to advise the Data Controller about GDPR, ensure compliance and protect all the data the practice holds. For more information about this please go to **Blog 3 in the Drop Box (see link below).**

The GDPR uses Privacy Notices (PNs) to tighten up the protection of individual data. Currently when individual data is processed it is generally good practice to inform them about it, but is not mandatory. Under GDPR, individuals have the right to be informed and therefore it becomes a strict legal obligation for us, the data controllers to inform people if we are processing their data and why. This right applies even if we have a sound legal standing for processing their data. For more information please go to **Blog 4 in the Drop Box (see link below).**

Now, by far the most interesting thing to come out of the GDPR is about consent. GDPR creates a lawful basis for processing data when it is for the provision of direct care stating that, to be lawfully processed does not require explicit consent, just implied consent. Explicit consent is when a patients literally asks for it via a form or verbally. Implied consent on the other hand is consent which is not expressly granted by a person, but rather implicitly granted by a person's actions and the facts and circumstances of a particular situation (or in some cases, by a person's silence or inaction).

However, we can't just process the data. It has to rest on the legal bases that it is 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'. Mind blown. Employee workload can actually be used as a legal basis. If you don't believe me read the guidance from the BMA (see link below)

In summary, GDPR:

- Makes Practices 'Data Controllers'
- A Data Protection Officer must be appointed
- Data Controllers must legally provide Privacy Notices to data subjects. The information that should be included is what type of information you hold, what you're doing with it, why, who it goes to and what rights they have over it
- Implied consent can be a legal basis for processing data if it is 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'
- Compulsory that Data Controllers keep and maintain up-to-date records of the data flows from the practices and the legal basis for these flows
- Have data protection policies in place
- Legal requirement to report data breaches
- Significant increases in financial penalties for breaches and non-compliance
- Practices can't charge patients for access to their medical records

You should also get someone to read the BMA, ICO and IGA guidance on GDPR at the bottom of this page and definitely get someone to go to training. Just saying.

# Training

NEL CSU will be delivering a GDPR training sessions on the following dates.

*Please note that this training is two parts, you must attend BOTH days*

| Date | Time | Venue |
|---|---|---|
| 26 April 2018 | 1.30pm – 4.30pm | Tower Hamlets Local History Library and Archives 277 Bancroft Road, London E1 4DQ |
| 22 May 2018 | 1.30pm – 4.30pm | Tower Hamlets Local History Library and Archives 277 Bancroft Road, London E1 4DQ |

This training session is targeted at Information Governance Leads and will cover:

- General Data Protection Regulation 12 steps overview, focusing on how it applies to healthcare and differences with direct care and research
- How to review your Information Assets Register to ensure it is GDPR compliant
- Lawful basis for processing
- Guidance on consent including children
- Guidance on Privacy Impact Assessments, how and when to do them
- The Subject Access Request Process under the General Data Protection Regulation
- The role of the Data Protection Officer
- Q&A session

- These sessions will provide you the opportunity to gain further insight into GDPR and ask questions to the Information Governance trainer.

Please **CLICK HERE** to register

# Useful Links

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

BMA: https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/gps-as-data-controllers

IGA: https://www.dropbox.com/referrer_cleansing_redirect?hmac=AGxVRrDCD0jhaEKZxfMATY41yslNhndJh2yfF4CRhUk%3D&url=https%3A%2F%2Fdigital.nhs.uk%2Fmedia%2F37922%2FIGA-GDPR-GP-Advice-Note-v1-FINAL%2Fpdf%2FIGA_-_GDPR_GP_Advice_Note_-_v1_FINAL

If you want to know even more about GDPR, you can read about it on a Drop Box. This is written in blog posts and are much easier to understand than the above. Here's the
link: https://www.dropbox.com/sh/h22kak6pxlt8ily/AAB4gAuHKib_MZ44Xi3AbAf4a?dl=0

Many thanks to Alex for having so nicely tried to demystify GDPR for us with his summary – hopefully the training will cover any remaining gaps, and we can get back

to talking about quality and stuff like this gorgeous weather next week.