Londonwide LMCs
The professional voice of London general practice

Data security and the General Data Protection Regulations (GDPR) - get ready now!

Earlier this month that the Government announced that the forthcoming European privacy rules set out in the General Data Protection Regulation (GDPR) will come into British law and update the existing Data Protection Act. This impacts on everyone, including GP practices.
The announcement confirmed that the EU’s GDPR will become active in this country, irrespective of what happens with ‘Brexit’.
Practices need to act now ahead of the GDPR coming into full force on 25 May 2018. It is arguably the most important data legislation change of recent times and the task of keeping data safe is now more vital than ever before.
What can practices do to prepare for the May 2018 deadline?
Practice Index have come up with the following advice:

Don’t panic There is no need to fear the GDPR. Many of its main concepts and principles are much the same as those in the current Data Protection Act (DPA). If you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR. This is a good starting point on which to build. There are new elements and significant enhancements, so you will have to do some things for the first time and some things differently. A good starting point is the Information Commissioner’s Office’s (ICO) helpful 12-step guide to get you started.

Learn what’s covered According to the main GDPR website, the regulations apply to personal data. This includes: names, photos, email addresses, bank details, posts on social networking websites, medical information and computer IP addresses. It is therefore vitally important to ensure that you collect and store confidential data and client contact data in accordance with the GDPR. This doesn’t mean that you should discard any data that has not been gathered with a GDPR compliant process. However, you must contact those individuals again to request the appropriate consent. If you work with children, you will need to gain parental or guardian consent in order to process their data lawfully.

Learn the basic principles According to the ICO, the GDPR centres around ‘controllers’ and ‘processors’. Effectively, the controller says how and why personal data is processed and the processor acts on the controller’s behalf. The GDPR places specific legal obligations on processors. eg, they are required to maintain records of personal data and processing activities and will have significantly more legal liability if they are responsible for a breach. These obligations for processors are a new requirement under the GDPR so you will need to make sure you are up to date with them.

Be proactive! Central advice on how the GDPR will affect centralised databases and the users of them in the NHS seems to be scarce at the moment. Be proactive if you have yet to receive any advice and ask for the information you need, finding out what you need to do early will be extremely helpful.

Get everybody on board GDPR and data protection requires buy-in from everyone in the practice team. It is likely that meeting GDPR needs will also involve changes to processes, so getting people onside will aid with change management. Understanding the tasks involved will also be vitally important.

Appoint a DPO (Data Protection Officer) You may need to appoint a dedicated DPO, who will be responsible for GDPR compliance. You will also need to ensure that everybody is clear as to their rights and responsibilities in relation to processes and procedures.

Understand your data Once you’re ready to make a start in ensuring your practice is GDPR compliant the first stage is all about understanding

your data. What data do you hold? How do you collect it? Where and how is that data stored? Who has access to it? How is the data currently used? Try to be as clear and as detailed as possible.

Compare The ICO recommends that once you understand what your current data set-up is like, you compare it against the GDPR requirements. This will help you identify any gaps in your processes.

Rights and requests One of the key elements of the new law is all about individuals’ rights – including the right to be forgotten. You will need to check your procedures to ensure they cover all the rights that individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. You should also update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

Plan for the worst The threat of cyber attacks is growing. As NHS organisations are a prime target for attack, it’s highly likely that GP practices will be the next victims. Plan for the worst and use a ‘when it happens’ not an ‘if it happens’ approach to dealing with a cyber attack. The GDPR states that you must inform the relevant authorities (ICO and NHS) of a data breach, within 72 hours of becoming aware of the breach. The information must include:

the types of data that were leaked
the number of registered parties the leak involved
the consequences of the breach to those registered parties
what has been done to ensure that the breach does not happen again
the methods of informing the data leakage – public announcement, personal letter or emails.

Make it an ongoing task
Data privacy and compliance with the GDPR is not a short-term obligation. Ongoing monitoring and compliance will be essential. This is where a DPO really comes into their own. The DPO will be vital in ensuring processes do not get ignored and good practice is followed at all times.

Overall, the GDPR will be an admin burden for practices, but in so many ways it’s all about processes and procedures and isn’t as daunting as it perhaps seems at first glance.
This information was produced with the kind permission of Practice Index, an organisation set up to support GP Practice Managers at medical practices throughout the UK. Visit https://practiceindex.co.uk/gp/ for further information.