Primary Care and the GDPR

Antonio Fletcher
Senior Associate
01622 776467
antoniofletcher@brachers.co.uk

Julie Alchin
Associate
01622 776467
juliealchin@brachers.co.uk

The General Data Protection Regulation ("GDPR") presents the biggest change to data protection laws in 20 years. Currently a new Data Protection Bill is making its way through Parliament to bring the GDPR into our domestic law and replace the Data Protection Act 1998. These new regulations will take effect from 25 May 2018 and now is a crucial time for primary care providers to ensure that they are prepared for the changes.

Due to the sensitivity of the data which they hold, many practices have a good level of understanding of their obligations under existing legislation compared to other sectors. However, now is not the time to be complacent as the changes being introduced by the GDPR are far-reaching, comprehensive and damaging (financially and reputationally) if they are not complied with.

Practices need to be wary not only of the highly sensitive data that is stored in relation to patients but also other personal data which the practice holds, some of which may also be highly sensitive – for example data regarding its own employees.

Many (if not all) members of staff within a practice will have access to much of the personal data the practice holds. It is therefore crucial that staff receive clear and comprehensive training regarding how they manage and process personal data (as the GDPR places an onus on employers to ensure that data is not processed by any other person save as instructed) and how they can identify and report breaches of legal requirements quickly.

The GDPR places a new requirement on organisations to report most breaches to the Information Commissioner's Office ("ICO") without delay (where feasible within 72 hours). In high risk situations the data subject must also be informed directly without delay.

Practices will also need to hold data protection at the forefront of their mind at all times, and particularly at the time of determining the purpose of the processing and at the time of processing the data itself. This will include integrating appropriate safeguards, using pseudonyms where possible and keeping the data processed to a minimum. Given the sensitive nature of the data being processed by providers of primary care, even smaller practices will be expected to have robust systems in place.

Individuals will also have enhanced and new rights in a number of areas including in how they are able to access data practices hold about them, having incorrect data rectified, restricting the processing of their own personal data, objecting to the processing of their personal data in some circumstances and the right to data portability (being provided with personal data about themselves in an electronic format that can easily be sent to and used by other organisations).

Data subjects have the right to be informed of these rights, as well as additional information including how the data will be kept and used, for how long and to which external parties it will be passed on to via a privacy notice which is given at the time the data is obtained from them (or within at most a month if the data is obtained from a third party).

Primary Care and the GDPR

The introduction of privacy notices will place a huge additional processing burden upon primary care providers which does not currently exist.

Where data is processed (e.g. text reminders for appointments) by reason of the subject having given their consent it is also important to be able to trace back that consent to ensure that it was "freely given, specific, informed and unambiguous" and was given by means of "a statement or by a clear affirmative action".

Where this cannot be shown, new consent will need to be obtained before 25 May 2018. However, consent is not the only basis on which to justify the processing of personal data (including sensitive personal data). Practices should consider the other lawful bases on which processing such data can be justified in compliance with the GDPR. Whatever the reason, this will need to be documented so that a practice can demonstrate to the ICO which lawful basis under the GDPR it is relying on.

The first tasks for practices are to gain a sufficient level of awareness of the GDPR and to carry out a full audit of their systems (electronic and manual) to gain an understanding of what data is held, how it was obtained and why it is being stored and/or processed.

Once a level of clarity has been achieved in this respect, the next steps will be to consider areas of risk and implement procedures that will ensure compliance from 25 May 2018 and will avoid the risk of substantial fines (up to £17m or 4% of group global turnover if greater) that are attached to the new regime.

If you have any questions about GDPR or compliance with data protection law, please contact Antonio Fletcher or Julie Alchin from Brachers' specialist Primary Care team.

Brachers
With you all the way

www.brachers.co.uk
01622 690691

Head Office
Somerfield House
59 London Road
Maidstone
Kent ME16 8JH

@brachersllp

Brachers LLP