Planning ahead: the impact of the GDPR on clinical trials in the EU

Careful forward planning is required by pharmaceutical companies conducting clinical trials ahead of the implementation of the General Data Protection Regulation in May 2018.

The new General Data Protection Regulation (GDPR) will become effective in 2018 in all EU Member States. Although it is expected that the GDPR will provide consistency across the territory of the EU, there are more onerous requirements concerning consent and the obligations on Data Controllers. Careful forward planning is required by pharmaceutical companies and CROs to ensure that future clinical trials are compliant, and to avoid any requirement to make retrospective amendments to consent forms and other clinical trial documentation.

2018 is set to be a busy year for pharmaceutical companies engaged in clinical studies in the EU with both the new Clinical Trials Regulation and the GDPR coming into effect. The GDPR (Regulation (EU) 2016/679) will have direct effect from 25th May 2018 without any transitional period, replacing the existing data protection framework under the EU Data Protection Directive. One of the drivers for a new regulation has been the advancement of technologies enabling the collection and use of data and the increasing use of the internet and electronic records. Furthermore, the use of “big data” (the combination of very large and diverse data sets) is becoming increasingly important in clinical research. All of these issues pose new challenges for data security and privacy.

The emphasis of the GDPR is on transparency, security and the accountability of Data Controllers whilst standardising and strengthening the protection of personal data across the EU. In short, the GDPR aims to strengthen the rights of individuals to be better informed about how their data is to be used, and sets out clearer responsibilities and obligations on healthcare professionals and companies using such data. Both health and genetic data are considered to be “Special Categories” of personal data, having enhanced control requirements requiring specific consent.

Although many of the concepts and principles are shared with those of the existing UK Data Protection Acts of 2008 and 2003, the GDPR strengthens requirements in some areas and introduces new obligations in others. The GDPR also gives data protection authorities more robust powers to enforce non-compliance with fines of up to 4 percent of annual global turnover for the most serious of breaches. There are also provisions that will make it easier for individuals to bring claims when their data privacy has been breached and to obtain compensation from Data Processors when they have
suffered non-material damage as a result of an infringement. Finally, the GDPR strengthens IT data security requirements. In particular, organisations are encouraged to consider "privacy by design" when building IT platforms to collect, process and store data.

Key points and recommendations:

- **Consent.** Consent remains at the centre of the GDPR as the legal basis by which personal data can be processed. Consent must be specific to each data processing procedure. Such consent must be "explicit and unambiguous" and must be freely given. Therefore, the data obtained cannot be used for any purposes except those clearly indicated on the consent form. Under Article 9 of the GDPR, the use of genetic material, biometric data, and data revealing racial or ethnic origin of trial participants constitutes the processing of sensitive personal data and requires specific consent. Trial participants should also be told on how they may withdraw their consent before it is actually given.

- **Transfer of data outside the EU.** The GDPR requires that all data regarding EU citizens that is transferred to destinations outside the European Economic Area (EEA) should be protected in a manner that is consistent with how personal data is protected in the EEA. Consent forms should specify that data is being sent outside the EU.

- **Data Protection Officer (DPO).** A company sponsoring a clinical trial and processing personal data will be considered a Data Controller under the provisions of the GDPR and so should ensure that a DPO is appointed in the EU to monitor compliance.

- **Accountability.** In contrast to the existing Directive, Article 30 of the GDPR requires that data controllers should be able to demonstrate their compliance and account and document for the action they have taken. Significantly, there are specific rules concerning the categorisation of data collected by controllers and the recordal of recipients to which the data is disclosed.

- **Pseudonymisation/anonymisation.** These are different concepts under the GDPR. Pseudonymisation provides only limited protection. The GDPR defines pseudonymisation as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information". Therefore, any pseudonymised data that could still be attributed to a trial participant by the use of other information will be considered personal data. The terms should be distinguished in trial protocols, as only the anonymisation of data will ensure that the data is no longer considered to be personal data. The Data Controller will need to decide when it is appropriate to anonymise or pseudonymise data. A data processor agreement will need to be in place when any pseudonymised data is shared with third parties.

- **Joint Controllers.** Article 26 of the GDPR sets out the responsibilities and liabilities of parties as "joint controllers". It is important that both the sponsoring company and CRO understand the remit of their obligations and the potential for overlap in their respective roles, as the line between a sponsor’s responsibilities and those of the CRO can often be blurred.

- **Right to be forgotten.** Under Article 17 of the GDPR, a trial participant can at any time request that all of their data be removed “without undue delay”. This onerous requirement on the sponsor as Data Controller would require the identification and deletion of any data, whether stored by the sponsor, CRO, hospital or any other third party. The right to be "forgotten" cannot be waived in the consent form. Article 89 of the GDPR allows the EU or Member States to limit certain individual rights, when necessary, to enable scientific research. However, this is not intended as a loophole to collect data for other purposes.
It is still unclear how Brexit will ultimately affect the long-term fate of the GDPR in the UK. However, as the UK will continue to need a clear and effective data protection regime, pharmaceutical companies conducting trials in the UK and wider EU need to be "GDPR ready". Companies and organisations that are due to commence clinical studies that will extend beyond 25 May 2018 need to be aware of changes introduced by the GDPR and should plan accordingly.

Please contact the authors if you would like to discuss any of the issues raised in this article in further detail.

This document (and any information accessed through links in this document) is provided for information purposes only and does not constitute legal advice. Professional legal advice should be obtained before taking or refraining from any action as a result of the contents of this document.