Data Protection and Clinical Trial

The highly regulated nature of the pharmaceutical industry means that organisations within this sector are no strangers to the requirement to abide by the various strict rules and regulations throughout the lifecycle of drug discovery, testing and production. However, when thinking about privacy and data protection regulations, clinical trials are certainly where it is most pertinent. Due to the volume of sensitive personal data that needs to be processed to demonstrate the safety and efficacy of a drug, this creates the requirement for significant data protection considerations. For clinical trials involving individuals located within the EU or UK, the General Data Protection Regulation, widely considered to be the 'gold standard' for safeguarding individuals' personal data, will be at the centre of such considerations. And, due to the GDPR's applicability being determined by the location of the individuals whose personal data is being processed and not the location of the entities doing the processing, trial sponsors located anywhere in the world are subject to the requirements set out within it.

In this article we set out four of the most important data protection factors that life sciences organisations must take into account when sponsoring a clinical trial that involves EU or UK residents:

- Basic data protection requirements
- Data transfers
- Local jurisdictional requirements
- Appointing a DPO and DPR

It is worth noting at the outset that following Brexit, the UK has enacted the GDPR into its own domestic legislation – the UK GDPR. At present, the EU and UK GDPRs are in practice the same, so unless stated otherwise, both will be referred to as the GDPR.

Basic Requirements

Data Controller

In all but very rare cases, trial Sponsors are deemed to be the 'Data Controller' under the GDPR for the personal data collected as part of a clinical trial. A Data Controller is the entity that determines the 'means and purposes for processing' personal data. Given the Sponsor is generally the organisation that writes the protocol (the purpose) as well as contracts with the various organisations that will run the trial and collect the data (the means), and even though the Sponsor may only have access to coded (pseudonymised) personal data, they are still considered the Controller under the GDPR. This means that as the Controller, Sponsors must comply with the more onerous accountability responsibilities required by the GDPR. This includes being responsible for identifying the appropriate lawful basis for the processing, implementing appropriate agreements to legitimise cross boarder data transfers, informing individuals about the intended processing, dealing with individuals' rights requests and ensuring the organisations you appoint as your Data Processors comply with their own obligations and apply 'appropriate technical and organisations measures' to protect the data being processed.

Lawful Basis

The first principle of the GDPR states that personal data must be processed lawfully. Therefore a lawful basis must be identified for each processing activity. Article 6 of the GDPR sets out the six lawful bases that organisations can choose from. In the context of a clinical trial, most sponsors can rely on 'Legal Obligation' to process data for reporting and safety reasons. However, for the main research purpose of a study, the three most common lawful bases to rely on are:

- Public task
- Consent
- Legitimate interest

The one that is the most appropriate will depend upon the context. Where a trial is commissioned by a public/government body, Public Task may be appropriate. If Public Task does not apply, sponsors will have to choose between Consent and Legitimate Interest and, depending on where data subjects are located, it could be different. In the UK for example, the preferred lawful basis is Legitimate Interest. However, in Germany the regulator requires Consent. It is therefore essential to investigate the specific guidance and rules within each different jurisdiction where trial participants are located, remembering that even Member States within the EU may differ on this point.

It is also worth noting that in many instances, personal data used in one clinical trial may also be used subsequently to benefit future research. Where this is the case, you will not need to identify an additional lawful basis for this additional research provided that the purpose of the additional processing is compatible with the purpose for which the data was originally collected. Recital 50 of the UK and EU GDPRs indicate that "Further processing for... scientific or historical research purposes... should be considered to be compatible."

Similar to a lawful basis, where health data is being processed, as is the case for most clinical trials, an additional condition for processing must be identified. This is because under the GDPR, information relating to things such as an individual's health; genetics; and sex life are considered 'special category data' and thus are afforded extra protections under Article 9 GDPR.

Data Protection Impact Assessments

Another requirement that falls at the feet of sponsors is the need to conduct a Data Protection Impact Assessment (DPIA) to assess the risks of the personal data processing involved in a clinical trial and ensure that mitigations for identified risks are in place. This is an essential step in demonstrating a trial's compliance with data protection laws, which is a key part of complying with the GDPR's Accountability principle.

International Data Transfers

As mentioned above, a sponsor may be subject to the GDPR even if it is not itself located within the EU or UK, but your trial participants that reside within these jurisdictions. Similarly, other vendors involved in the trial may also be located outside of the EU/UK but still subject to the GDPR, such as your Contract (or Clinical) Research Organisation (CRO). Therefore, the personal data of EU/UK individuals may be transferred to countries outside of this area (known as third countries). Where this is the case, the GDPR requires that an appropriate transfer mechanism be put in place to safeguard the personal data being transferred and ensure that it is protected in an 'essentially equivalent' manner to if it had remained within the EU/UK.

Currently, 14 countries (including Argentina, Canada, Israel, Japan and New Zealand etc. – but not including the US), have been deemed 'adequate' by the European Commission (and the ICO for the UK), meaning that the laws in these countries have been deemed to provide a level of protection of personal data that is 'essentially equivalent' to that provided by the GDPR. This means that data can flow freely between these countries without the need for further safeguards. The EU and UK have also granted each other Adequacy.

Given most countries have not been granted this status, organisations making personal data transfers to these countries (most notably, the US) must ensure that additional safeguards are in place. In most cases, in the EU context these safeguards come in the form of EU-specific Standard Contractual Clauses (EU SCCs) that need to be included within an agreement between the sharing organisations. The EU SCCs guarantee rights and protections for data subjects when their data is being transferred to a third country. If your organisation is exporting data from the UK, to a non-adequate country, you cannot rely on SCCs and should instead rely on either the UK's Addendum to the EU SCCs or the UK-specific International Data Transfer Agreement (IDTA). In addition, organisations relying on EU SCCs (or the UK equivalent) to transfer personal data, must now complete a Transfer Impact Assessment prior to the sharing commencing. A TIA is used as a mechanism to assess the laws of the importing entity's country and consider whether the risks posed by the non-adequate jurisdiction can be adequately mitigated.

Whilst the above is currently virtually the only way to transfer personal data to the US, there is potential for a new international agreement that could see transfers become easier. The US and the EU are at present in political talks to create a new Trans-Atlantic Privacy Framework, which would allow for the seamless flow of data between the EU and the US. In October 2022, President Biden signed an Executive Order to help with putting this agreement in motion. The UK, since it has left the EU, would need to create its own agreement with the US, but may well follow the EU's lead in the near future.

Jurisdictional Requirements

If conducting a trial involving multiple investigator sites located in different countries, it is important to be aware that there will likely be varying data protection requirements (beyond which lawful basis to select) affecting each location, even if all locations are within EU Member States.

The Clinical Trials Regulation (CTR) that came into force in the EU in early 2022 did go some way to harmonising the rules in this area, and the new Clinical Trials Information System (CTIS) that is set to become mandatory for trial applications in the EU from January 2023 will go further to achieve this and making it easier to run trials across multiple Member States. The CTR allows Sponsors to submit one application, via the CTIS portal, for approval to run the trial in multiple Member States. To gain approval, life sciences organisations will need to provide a statement on their compliance with the GDPR and any other local jurisdictional requirements. The Sponsor then declares this on the CTIS submission.

However, despite these recent changes, sponsors still need to be aware that jurisdiction-specific requirements are very much still relevant in some countries. For example, any trial involving French residents must submit an MR-001 declaration form, to demonstrate that the Sponsor has developed a robust data protection framework, has completed a DPIA, and that they have appointed an EU Data Protection Representative (DPR). The CNIL, the French Data Protection Authority, has also released specific guidelines on personal data processing in clinical trials, including a requirement that only anonymised or pseudonymised data can leave the EU, with the anonymisation/pseudonymisation occurring before export.

As a non-EU country, the UK is not party to the CTR or CTIS. The clinical trial regulator for the UK is the Medicines and Healthcare Products Regulatory Authority (MHRA). For the data protection requirements related to trials conducted within the UK, sponsors must look to the UK GDPR, the MHRA's requirements and any additional rules and guidance from the Information Commissioner's Office (ICO).

Data Protection Officers (DPO) and EU/UK Data Protection Representatives (DPR)

Life sciences organisation conducting trials in the EU or UK must appoint a DPO. A DPO's role is to inform, advise and monitor compliance with data protection legislation. This involves assisting with the carrying out of DPIAs; undertaking Data Processor (vendor/supplier/partner) due diligence and ensuring the required agreements are in place; creating policies and procedures to maintain compliance; responding to individuals' rights requests, such as data subject access requests (DSARs) and requests for deletion, and maintaining other required documentation.

In addition to a DPO, an EU and/or UK Data Protection Representative (DPR) is required when a Sponsor does not have a presence with the EU/UK but processes the personal data of individuals located within these areas. The Representative must be established in one of the countries where the processing is taking place and act as a point of contact for the regulatory authorities and for the data subjects. If your trial is being conducted in multiple EU Member States, you will only need one DPR, ideally located in the country where the largest proportion of data subjects are located. But, if your trial takes places in the UK and EU, you will need two separate Representatives – as per Article 27 of UK and EU GDPR.

Contracts and Agreements

A final consideration to note is that as data controllers, clinical trial sponsors will need to ensure that they have implemented appropriate contracts and agreements with each third party involved in the processing of the trial's personal data. These will include:

- Data processing agreements – Under Article 28 GDPR, this type of agreement is required between a Controller and Processor. These agreements set out the Processor's obligations including the mandatory reporting of breaches to the Controller; retention of data upon termination of the contract; and any audit rights the Controller has over the Processor. These types of agreements would normally be implemented with your CRO and laboratories

- Joint controller agreements – If Sponsors intend to share the role of Controller with another entity (i.e. jointly determining the means and purpose of processing the trial data), a Data Sharing Agreement setting out the responsibilities of each party in relation to the personal data being processed must be in place. These types of agreements may be implemented with your investigator sites

Conclusion

Conducting a clinical trial within the EU and/or the UK brings with it a number of data protection considerations that must be accounted for. Appointing an experienced DPO will help to ease this burden by guiding the sponsor through the relevant obligations to ensure compliance. It is vital for trial sponsors to ensure that they fully understand their data protection obligations in the EU and UK because, ultimately, this could lead to trial delays or failure to gain approval.

Rob Masson

As founder and CEO of The DPO Centre, Rob is actively driving innovation, transformation and thought leadership in data protection and privacy. For over 30 years, Rob has been involved in delivering solutions to some of the world's largest and most respected organisations. Supported by the DPO Centre's large team of privacy professionals, Rob advises on evolving data protection legislation and how, when implemented well, compliance builds trust, confidence, loyalty and engagement. The DPO Centre assists a broad range of bioscience, genomics, therapeutics, healthcare and pharma companies globally to comply with EU data protection laws such as the GDPR.