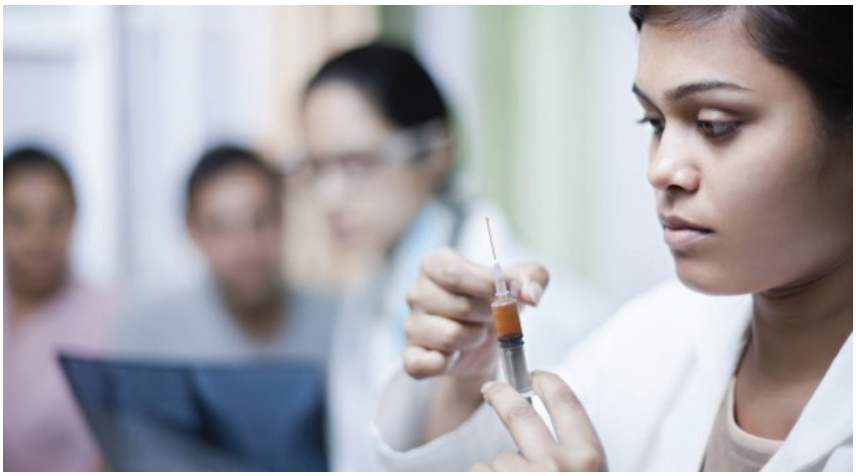
MARSH

INSIGHTS | MAY 2019

Drug and Device Clinical Trials and the GDPR

Clinical trials are a critical and fundamental part of all life science companies' operations. Data management, security, and privacy within clinical trials are important, but they're complicated.



They're complicated because of:

- the number of parties who provide, handle and process data including "personally identifiable information".
- the increasing use of the internet, electronic records, and the advancement of clinical trial technologies that enable the collection and use of data.
- the increasing importance of "big data" in clinical research.

In this article we will discuss the implications of the changing regulatory landscape for all players within the clinical trial supply chain.

Not all regulations are the same

The various rules, regulations and laws that govern clinical trials do not have the same level of authority in all countries or regions, or take a coordinated approach. To add to this complexity, data privacy laws across geographies can apply independently and simultaneously to a "breach", making the legal situation even more challenging.

The role of the GDPR

The European Union's (EU) *General Data Protection Regulation* (GDPR) is the most important change in data privacy regulation in 20 years. It came into force on May 25, 2018, from which time any organization that does not comply may face heavy fines. (The European data protection authorities have the power to levy discretionary fines of up to 4% of an organization's global revenue or €20 million, whichever is greater.)

The GDPR is designed to harmonize data privacy laws across Europe, protect and empower all EU citizens' data privacy, and reshape the way organizations approach data privacy. It expands the type of companies that need to comply with it, strengthens data subjects' rights, and raises the bar for security and privacy.

The role of the GDPR with respect to clinical trials data

The GDPR sets out clearer responsibilities and obligations on healthcare professionals and companies using individuals' data. Transparency, security, and the accountability of data controllers are paramount.

Critically, clinical trial providers, wherever they reside, must identify the data that is being processed, where it is transferred to, who processes the data, what it used for, any risks and processes, and ensure all employees are trained to understand their GDPR responsibilities.

What are the key GDPR provisions relevant to clinical trial providers and processors?

- Extra-territorial effect– the GDPR's scope is broad.
- Consent is required for data handling, storage and processing.
- The accountability principle is applied to controllers and processors and "privacy by default" and "privacy by design" principles are introduced.
- New rights for the data subjects (for example, right to: "be forgotten"; data portability; data access; data correction, and to restrict data).
- Privacy impact assessment responsibility for data controllers.
- Increased control and sanction regime.

So who is responsible for what in the context of a clinical trial?

Many of the responsibilities and obligations defined by the GDPR are not new for companies in the clinical research sector. Ethics committees attached to almost every clinical trial demand that subjects sign an informed consent form before being part of the trial process.

What's new is the requirement to also obtain consent with respect to data handling, storage and processing.

For clinical trial providers (a "processor" from a customer point of view and a "data controller" from a personnel, salespeople and subcontractor perspective), the new regulations cover not only those participating in clinical trials, but also employees, customers, and subcontractors which can include contract research organizations (CROs), investigators or statisticians.

Let's look at scenarios and some implications to demystify the confusion

Scenario 1:
The trial site is in the EU. The trial subjects are EU citizens. Neither the sponsor nor the CRO are in the EU.

The GDPR applies - irrespective of where the sponsor and CROs/vendors are located, where the data processing is performed, or where the data submission is planned. It's enough that the trial subjects are in the EU.

It would also apply if the subjects were not EU citizens but their data was collected while they were in the EU.

Furthermore, a sponsor who is not based in the EU but who is processing data from data subjects within the EU must nominate a representative within the EU who will fulfil their responsibilities with respect to the GDPR.

Scenario 2:
The trial site is not in the EU. The data subjects are not in the EU. The sponsor is based in the EU.

The GDPR will apply in this situation because the sponsor will process the data in the EU.

Scenario 3:
The sponsor is not based in EU.

The GDPR rules may apply if:

- data collection, or data processing occurs in the EU.
- if a joint controller is in the EU.
- it is the intention of the sponsor to support a market authorization filing in the EU.
- a full service CRO based in the EU involved in all or part of the trial.

These scenarios may get even trickier with device trials, especially wearable devices that collect and process data.

For example, if a trial subject went on a 10-day work trip to the EU wearing a device, the GDPR rules would apply with respect to the data collected during that time.

Managing the exposure: risk considerations

Trial sponsors and associated parties obligated under the GDPR, should think through the potential trial scenarios and evaluate their risks under each.

Importantly, many well designed contracts between CROs and sponsors now include a clause requiring compliance with the GDPR as a prerequisite. However, most sponsors don't know if they should be accepting the liability being transferred to them, and to what extent or how, the laws apply - especially if the links to Europe seem tenuous.

What actions should insurance buyers take now?

As the requirements of the legislation become clearer and regulators implement the new rules, your risk profile may have changed.

Key considerations include:

- How can you assure compliance with, and preparedness for, the GDPR across your supply chain?
- Have you assessed the insurability of GDPR fines in the geographies in which you operate? The type of non-compliance, and what insurers are open to will vary from country to country.
- Have you considered using surety bonds for financing any potential fines?
- Have you undertaken a cyber risk assessment, quantified that risk, and considered how you will mitigate or transfer it?
- Have you built provisions into your supply agreements to account for the GDPR and any failures to comply?
- Have you performed a vulnerability (revenue impact) assessment for non-compliance across your supply chain?
- Whether your business interruption policy can be extended to include "non-damage triggers" such as regulatory breach for your business or your major suppliers.
- The potential for management to be held personally responsible if the company fails to comply with the new regulations. Check whether your directors and officers policy will respond to litigation from stakeholders alleging breaches of your governance duties.
- Ensure adequate product liability and clinical trials liability are in place and meet "sufficient financial coverage" requirements.

We recommend working with your advisers to:

- Understand your policy wording.
- Review limits for adequate coverage of all costs of GDPR non-compliance including:
  - Forensics.
  - Breach notification.
  - Breach support services.
  - Legal liability to impacted subjects.
  - Legal and regulatory defense costs.
- Seek policy wording that maximizes your potential recovery.

For more information about Life Sciences and other solutions from Marsh, visit marsh.com, or contact your local Marsh representative.

PRASHANSA DAGA
Life Sciences Industry Leader
+65 8318 3753
prashansa.daga@marsh.com