SOCRA® FOR CLINICAL RESEARCH EXCELLENCE

SOURCE

JOURNAL FOR CLINICAL RESEARCH EXCELLENCE

A publication of the Society of Clinical Research Associates

November 2023 | Issue 118

HIGHLIGHTS IN THIS ISSUE

QUALITY EDUCATION

PEER RECOGNITION

CLINICAL RESEARCH CERTIFICATION

NCCA ACCREDITED PROGRAM

SOCRA® FOR CLINICAL RESEARCH EXCELLENCE

Society of Clinical Research Associates
530 West Butler Avenue, Suite 109 Chalfont, PA 18914 USA
Phone: (215) 822-8644 | Fax: (215) 822-8633
Email: office@socra.org | www.socra.org

Rob Masson

Considerations for Clinical Trial Sponsors Processing E.U. and U.K. Personal Data

Rob Masson, CEO

The DPO Centre Ltd

Abstract: *Compliance with European Union and United Kingdom data protection regulations and requirements is one of the most important issues clinical trial sponsors in the United States need to consider when acting as the data controller for personal data collected from clinical trial participants in the European Union and the United Kingdom. This article covers the impact of the Clinical Trials Regulation, the introduction of the Clinical Trials Information System, the requirements around European Union and United Kingdom representation, and the considerations for cross-border data transfers.*

Data Protection Overview

Data protection has become a huge issue for organizations handling medical and health data, especially those conducting clinical trials. Data protection laws have been around for decades, and the medical and health sector is no stranger to compliance, however it was still a game changer when The European Union (E.U.) General Data Regulation (GDPR) came into effect in 2018 (Table 1).

The E.U. GDPR imposed significant penalties for non-compliance and the seventh principle introduced a requirement to be accountable for the personal data processed. Also, the E.U. GDPR expanded the concept of extra-territorial scope to data protection law. Essentially, this means the law applies to any organization globally that is processing the personal data of E.U. data subjects (any individuals in the EU/EEA). Therefore, life sciences organizations based in the United States, for example, are required to comply with the E.U. GDPR if their clinical trial participants reside within any of the 27 E.U. Member States.

TABLE 1
The E.U. GDPR

- Imposed significant penalties for non-compliance
- Requires accountability for processing personal data
- Applies to any organization globally that is offering goods and services to
  or otherwise monitoring the behavior of, personal data on E.U. data subjects
- Data controller:
  - Determines the means and purpose of processing
  - The sponsor
- Data processor:
  - Processes personal data on behalf of a data controller
  - Includes the CRO
- Accountability for demonstrating compliance
- Informed consent forms and ethics committee submissions:
  - Should include confirmation of compliance in the privacy notice

The obligations set out in the E.U. GDPR apply to any organization legally considered to be a data controller or a data processor. A data controller determines the means and purposes of processing personal data and a data processor processes personal data on behalf of the data controller.

In the context of a clinical trial, the sponsor is the data controller and, as an example, an organization such as a contract research organization (CRO) is likely to be considered a data processor. Depending on their level of input in executing the study protocol, however, the CRO might occasionally be considered a joint data controller along with the sponsor. This is becoming more common when CROs do everything except writing the protocol. This is but one of many idiosyncratic complexities that arise within clinical trial data processing.

Sponsors must be able to demonstrate accountability for any personal data being processed. They must ensure all parties within the data supply chain have implemented appropriate technical and organizational measures to adequately protect the data. Also, they must ensure any appropriate controls and safeguards necessary to legitimize international data transfers are in place.

As a data controller, all these requirements apply, regardless of whether the sponsor ever sees participant identifiable data or not. The necessary compliance framework to meet these requirements consists of a range of policies, including the privacy notice. The privacy notice describes the intended data processing, how participants' personal data will be collected, shared, and protected, and the retention period. Privacy notices are required to ensure compliance with E.U. GDPR's transparency requirements

Sponsors do not necessarily need to be able to see identifiable data to be considered the data controller. In many cases, data provided to the sponsor is anonymized or pseudonymized, and clinical trial participant identifiable data is not visible. However, since the sponsor, has requested the data to be collected and collected for a specific reason, the sponsor is defined as the data controller as they are determining the purpose and means of processing. In contract, the CRO is generally considered the data processor wherever the CRO is collecting the personal data under the sponsor's instructions.

Other personal data of E.U. and United Kingdom (U.K.) data subjects might be processed during a clinical trial. This could include personal data about investigators and site staff, vendors, and sponsor employees. As the data controller, the sponsor must ensure personal data are processed according to the seven E.U. GDPR principles. Appropriate technical and organizational measures must be implemented throughout the data supply processing chain and the personal data must be processed in accordance with the laws.

A key requirement of the seven E.U. GDPR principles is accountability. This requires data controllers to demonstrate compliance with the other six principles. Sponsors must implement a compliance framework consisting of policies and procedures, registers, log files, legal agreements, and risk assessments prior to the collection of any personal data.

Confirmation of compliance with these requirements should be articulated in the privacy notice, which is often integrated into the informed consent forms and within ethics committee submissions. Recently, it has become more common for ethics committees in Member States' to request detailed data protection impact assessments to be submitted along with the clinical trial application submissions. Compliance with data protection laws is a key requirement of the pre-trial phase. Non-compliance can be a significant potential roadblock standing in the way of successful and timely clinical trial set-up and initiation.

Processing Personal Data of Clinical Trial Participants in the E.U. and the U.K.

Table 2 provides an overview of processing personal data in the E.U. and the U.K. Medical and health data are classified as special category data under Article 9 of the E.U. GDPR. Sponsors are subject to much stricter obligations to protect and secure special category data throughout the data processing chain and its lifecycle.

TABLE 2
Processing Personal Data in the E.U. and the U.K.

- Demands greater protections
- Places more onerous demands on data controllers
- Requires an additional condition for processing Special Category Personal Data
- Data are often high risk:
  - Requires a Data Protection Impact Assessment
- Requires updated privacy notices and informed consent forms

Each participant, of course, is required to complete an informed consent form to confirm participation in the clinical trial and for the purposes of complying with the Clinical Trials Regulation. However, there is a difference between 'informed consent' within a clinical trial context and the lawful basis of 'consent' under GDPR; the latter may not be an appropriate lawful basis for compliance with the sponsor's requirements of the E.U. GDPR. The data controller is responsible for identifying the appropriate lawful basis for processing personal data under the E.U. GDPR.

Consent is one of six lawful bases available under Article 6 of the E.U. GDPR. In certain contexts, public interest, legitimate interest or legal obligation, may be a more appropriate lawful basis. The appropriate lawful basis depends upon the jurisdiction, the organization conducting the clinical trial, the data being collected, and why the data are being collected.

When considering a clinical trial, there are two types of data processing:

- To ensure the reliability and safety of the clinical trial
- For research purposes.

The lawful basis for data processing to ensure the reliability and safety of the clinical trial is already well established as being necessary for the sponsor's legal obligations under the Clinical Trials Regulation. The most suitable lawful basis for data processing for research is less clear and will vary from country to country. There is an ongoing difference of opinion throughout the E.U. and the U.K. over whether consent, legitimate interests, or even legal obligation is the most suitable lawful basis for data processing for research.

The U.K. Medical Research Council and the Information Commissioner's Office both argue that legitimate interest makes the most sense due to the difficulty in demonstrating consent is freely given. Freely given consent is a requirement under the E.U. GDPR. There are also complications in enabling clinical trial participants to withdraw their consent at any time. The European Data Protection Board took the same stance in a 2019 opinion. Despite this, a few Member States, including Germany and Austria, still mandate that consent is the lawful basis for almost all processing related to clinical trials.

The result of these contrasting approaches is that it is often difficult for sponsors to standardize their approach across jurisdictions, even without consideration of the other requirements for clinical trials that vary across these countries. Under the Clinical Trials Regulation, organizations must always obtain informed consent from clinical trial participants. This obligation, however, is unrelated to data protection laws. It should remain completely separate, even if consent is the lawful basis to be relied upon under the E.U. GDPR.

Under the E.U. GDPR, consent must be as easy to remove as it was to initially obtain. Where a data subject withdraws their consent for data processing, the sponsor no longer has a lawful basis for processing the Personal Data and must cease further collection and additional processing. That being said, all of the information that has been collected and processed to that point may be retained by the sponsor for further analysis. Other Data Subject Rights, such as the Right to Erasure, are explicitly exempted under the E.U. GDPR and national implementation legislation in certain circumstances involving scientific research.

Consent can only be requested in situations where there is a balance of power between the data subject and the data controller. It can be very difficult to argue that consent would be given without influence or coercion in a doctor-patient scenario. The doctor is in a strong position of trust and influence. The clinical trial is only available if the patient provides consent. Thus, if consent as the lawful basis for processing personal data is ever scrutinized, this could be a problem for sponsors.

For these reasons, consent offers a slightly less straightforward lawful basis for processing personal data. It remains, however, the lawful basis for data processing that some E.U. ethics and clinical regulatory bodies advise. Harmonization of the lawful basis for complying with the E.U. GDPR continues to be a major challenge for sponsors and their data protection officers.

When processing special category data, Article 9 of the E.U. GDPR requires an additional condition. Explicit consent is an option but not the only option. Other options include public health or scientific research purposes, which may be a more appropriate choice.

A vital element of meeting the accountability requirement is performing a specific exercise to identify and record the lawful basis for complying with the E.U. GDPR. In most cases, the mechanism used to identify and document the justification is called a data protection impact assessment (DPIA). This assessment is used to assess the risk associated with the data processing and consider what mitigation or adjustments might need to be implemented prior to starting data processing.

Transparency is also crucial. The sponsor must be clear, open, and honest with clinical trial participants from the start about how and why their personal data will be used. This requires updating privacy notices and informed consent forms before any personal data are collected.

The privacy notice and informed consent forms should include clear, transparent information about the personal data required, how they will be used, the categories of recipient of that data and how long the data will be retained. Also, the sponsor must provide adequate privacy notices to clinical research site staff during the feasibility process and the site initiation visit as well as including relevant information within employment contracts.

International Data Transfers

Data flows and cross border transfers of data are complex (Table 3). In July 2020, a five-year legal process between Austrian privacy activist Max Schrems, Facebook, and the Irish Data Protection Commission culminated in the Schrems II decision. The ruling by the Court of Justice for the European Union (CJEU) invalidated the privacy shield, which was one of the primary mechanisms that enabled the lawful transfer of personal data from the E.U. to the U.S. without the need to implement additional safeguards. The privacy shield was a self-certification scheme whereby each member organization confirmed that they complied with the principles and requirements of the framework.

At the same time, due to legal maneuvers by Facebook, the Court of Justice for the European Union also ended up calling into question a much more widely used global transfer mechanism known as standard contractual clauses (SCCs). The European Commission has since reissued updated standard contractual clauses that are designed to provide a mechanism to enable transfers of personal data from the E.U. to a third country. A third country is a country other than one of the 27 E.U. Member States and the three additional countries in the European Economic Area (Iceland, Liechtenstein, and Norway). Since Brexit, the U.K. is no longer part of the E.U. or the European Economic Area.

Personal data can only be transferred to third countries in compliance with the conditions for cross-border data transfers set out in the E.U. GDPR. Appropriate safeguards are required to enable transfers of personal data from the E.U. Member States and European Economic Area countries to third countries. If personal data are being transferred from the E.U. to a third country that has not been awarded what is called an adequacy decision by the European Commission, it will be necessary to determine which of the available data transfer safeguards must be put in place.

TABLE 3
International Data Transfers

- E.U. to U.S. data transfers:
  - Transfers are no longer covered by privacy shield:
    - Schrems II decision
  - EU-US Data Privacy Framework (DPF) launched in July 2023
    - Many life science organizations are yet to self-certify
  - Alternative safeguards can be used, such as standard data protection clauses
- U.K. to U.S. data transfers:
  - U.K. highly likely to enter into a similar DPF-type agreement with the U.S.
    - UK-US data bridge agreement in principle announced in June 2023
    - Requires final details and legislation passed to go into effect

Standard contractual clauses are the most likely data transfer safeguard to be used. These are part of a standardized legal document provided by the European Commission that is generally annexed into a larger agreement. The core terms of standard contractual clauses must always remain unchanged in order to remain valid. They are not negotiable.

Standard contractual clauses are designed to create a binding contract between the legal entities of the exporter and the importer. They impose requirements on the importer to ensure that 'essentially equivalent' protections will be implemented to protect the data compared to those imposed on the exporter by the E.U. GDPR while the data reside in the E.U.

As part of the Schrems II decision, the CJEU did not invalidate the standard contractual clauses active at that time. The court did rule, however, that additional measures would now be required to ensure data transfers were not subject to the foreign surveillance laws of foreign governments. As such, standard contractual clauses must be accompanied by a transfer impact assessment (TIA) to assess the risks associated with the transfer and what additional safeguards are required to mitigate those risks. The decision came with no grace period and no obvious alternative solutions.

This ruling has put the U.S. in the spotlight, primarily due to U.S. surveillance laws, such as the Foreign Intelligence Surveillance Act and Executive Order 12333, signed by Ronald Regan in 1981.

As of July 2023, E.U. and U.S. politicians have announced a new transatlantic data privacy framework (DPF). Some concessions have been made by the US Government in respect of the right to redress, however only minor changes have been made to U.S. surveillance laws, therefore it is difficult to see how this new agreement will stand up to the inevitable Schrems III challenge.

Given the freedoms that Brexit is now affording the U.K., the U.K. is also negotiating a similar DPF agreement with the U.S., described as an extension to the E.U. – U.S. DPF. This agreement in principle has been described as a 'data bridge' between the U.K. and the U.S., which would see U.K. data subjects be offered the same redress rights afforded to E.U. data subjects under the DPF.

However, it is possible that this arrangement, if it were to be based on reduced transfer requirements, may have a further negative impact on the European Commission's currently favorable adequacy decision with the U.K. This adequacy decision enables the free flow of personal data

between the E.U. and the U.K. without the need for additional safeguards, as the E.U. deems the U.K. to have essentially equivalent data protection laws to the E.U. Aside from the U.S. and the U.K., there are 13 other jurisdictions the European Commission deems to be adequate.

This ever-evolving area of law is creating a great deal of work for non-E.U. sponsors responsible for ensuring relevant standard contractual clauses are in place between themselves and any exporting body, either directly or through their CRO. It also ensures any non-E.U. processes, such as laboratory information systems, electronic master trial file providers, or other consultants, are covered by appropriate standard contractual clauses.

It is also becoming increasingly common for clinical research sites to request clinical trial data protection impact assessments and evidence of standard contractual clauses for all third parties prior to exporting data outside the E.U. The risks posed by the outcome of the Schrems II decision exist equally for the exporting site. It often falls on the sponsor to demonstrate compliance all along the clinical trial data flow before they can provide adequate assurances to investigators.

The Clinical Trials Regulations

In Europe, the key regulations governing clinical trials are the Clinical Trials Regulation, the U.K. Clinical Trials Regulation, and French regulations (Table 4). The Clinical Trials Regulation entered into application on January 31, 2022, replacing the Clinical Trials Directive. It is intended to harmonize the processes for assessment and supervision of clinical trials throughout the E.U. and to foster innovation in research and enable larger clinical trials to be conducted in multiple Member States and countries within the European Economic Area.

Prior to the Clinical Trials Regulation, sponsors had to submit separate applications to national competent authorities and ethics committees in each country to gain regulatory approval. The regulation enables sponsors to submit one clinical trial application through an online platform known as the Clinical Trials Information System (CTIS) to seek approval to run a clinical trial in up to 30 countries. This makes it considerably more efficient to conduct multi-national clinical trials. The Clinical Trials Regulation also allows national regulators to collaboratively process clinical trial applications in more than one country, request more information, approve or refuse a clinical trial, and oversee and authorize clinical trials.

As of January 31, 2023, sponsors must use the CTIS for new clinical trial applications.

Furthermore, as of January 31, 2025, any ongoing clinical trials already approved under the Clinical Trials Directive must comply with the Clinical Trials Regulation. Sponsors must have recorded information on their clinical trials into the CTIS by that date.

When submitting a clinical trial application through the CTIS, the sponsor must provide a statement on compliance with the E.U. GDPR in general and a statement on compliance with specific data protection laws, where necessary. This reinforces the requirement that E.U. GDPR compliance must be considered and implemented early when setting up the clinical trial, rather than assuming it can be addressed shortly before the processing of personal data begins.

On December 31st 2020 – known as IP (Implementation Period) Completion Day – the U.K., rather than try to rewrite 40 years of E.U. law overnight, decided to retain all E.U. laws as U.K. laws, including retaining the E.U. GDPR as the U.K. GDPR.

The current U.K. clinical trials law is The Medicines for Human Use (Clinical Trials) Regulations 2004 (as amended), which is based upon the older E.U. Clinical Trials Directive.

Now that the dust is settling on Brexit, the U.K. is free to adapt these laws to its own benefit. Both the GDPR and the Clinical Trials Regulation are currently subject to consultation processes. Amendments to both laws are likely and, therefore, the process and requirements are also likely to change. This may create a more complex environment for sponsors running clinical trials in both the E.U. and the U.K., as there will be separate processes and requirements. This is likely to add additional complexity and cost to the clinical trial process.

TABLE 4
European Regulation Related to Processing
Personal Data in Clinical Trials

- Clinical Trials Regulation:
  - Came into effect on January 31, 2022
  - Helped establish the Clinical Trials Information System:
    - Sponsors submit clinical trial information
    - Sponsors must provide a statement on compliance with EU GDPR
  - Required for new applications since January 31, 2023
  - Active clinical trials must be recorded by January 31, 2025
  - Sponsors are responsible for ensuring that:
    - The clinical trial is E.U. GDPR compliant
    - Relevant documents are uploaded
- U.K. clinical trial regulation post-Brexit considerations:
  - U.K. retains the E.U. GDPR as the U.K. GDPR
  - U.K. clinical trials law is The Medicines for Human Use (Clinical Trials) Regulations 2004
  - It is possible that U.K. GDPR may be amended via the 'Data Protection and Digital Information Bill (No 2)
  - For U.K. clinical trials, sponsors must follow:
    - U.K. GDPR
    - U.K. Clinical Trials Regulation
- Clinical trials in France:
  - Commission Nationale de l'Informatique et des Libertés and MR-001:
    - E.U. Clinical Trials Regulation and GDPR also apply
    - Sponsor must:
      - Submit self-declaration to MR-001
      - Confirm a suitable data protection framework
      - Provide details for the E.U. GDPR representative
      - Perform a data protection impact assessment
    - Commission guidelines for exporting data out of the E.U.:
      - Only anonymized or pseudonymized personal data can leave the E.U.
      - Anonymization or pseudonymization must occur before data transfer
      - Processors accessing identifiable data cannot access health data

France is no different than the other E.U. Member States in its adoption of the E.U. GDPR and the Clinical Trials Regulation. In July 2018, however, the French data protection regulator, the Commission Nationale de l'Informatique et des Libertés (CNIL), issued an update to the methodology known as MR-001, replacing the 2016 MR-001. MR-001 is a self-declaration process that allows data controllers processing personal data for the purposes of health research, and in particular clinical trials, to proceed without waiting for the lengthy approval process from CNIL.

This makes the process more seamless and supports the strict timelines normally associated with clinical trials. However, if the intended data processing falls outside the scope of MR-001, then explicit authorization is required from CNIL. Waiting for this approval may subject the clinical trial in France to lengthy delays.

The data controller must evaluate their processing of personal data prior to initiating the clinical trial and ensure they have a suitable data protection framework that meets the requirements of the E.U. GDPR. Sponsors unfamiliar with the complexities of these requirements, or those lacking the necessary skills or expertise, must appoint a data protection officer or legal counsel to assist with the framework set-up and to assist in an ongoing basis throughout the clinical trial. Where applicable, the data controller must specify the contact details of their E.U. GDPR representative.

Given some clinical trials consist of multiple processing activities, the data controller must consider performing compliance checks and a data protection impact assessment (DPIA) for each activity, as they may require different lawful bases.

CNIL has also provided specific guidance for exporting clinical trial data out of the E.U. The key requirements are anonymization or pseudonymization. Anonymization means the complete and irreversible removal of any information that could lead to an individual being identified either from the removed information or when the information is combined with other information. This would mean, for example, that not even the CRO or Site would know which participants the data are related to.

Pseudonymization means the processing of personal data must be done in such a manner that the personal data can no longer be attributed to a specific person without the use of additional information. For example, any personal data on a clinical trial participant can be exchanged for a participant reference number. The CRO or, more commonly the clinical research site, would continue to hold the necessary details to match the clinical trial participants with their participant reference numbers. Therefore, the data are only indirectly identifiable.

CNIL guidance states only anonymized or pseudonymized data can be exported from the E.U. The anonymization or pseudonymization process must be completed before the data leave the E.U. The commission further requires any sub-processes that access identifiable participant data must not be able to access health-related information. This has proven to be problematic when working on a clinical trial with a range of stakeholders, particularly in the area of participant reimbursement.

U.K. and E.U. GDPR Data Protection Representatives

Table 5 highlights the roles of the data protection officer and the data protection representative. The data protection officer generally provides the specific expertise necessary to implement these requirements and to draft the privacy notice. Also, the data protection officer will ensure the sponsor remains compliant with the E.U. GDPR and the data are processed appropriately during the framework set-up for a clinical trial and throughout its lifecycle. The E.U. GDPR only requires the appointment of one data protection officer regardless of the number of Member States where the clinical trial will be conducted. Conversely, the data protection representative, based within the E.U. or the U.K., acts in an oversight and subject matter expert capacity to comply with the data requirements and protect the interests of the sponsor.

All reputable CROs will be able to demonstrate their E.U. GDPR compliance. The CRO will collect, store, and process data in a GDPR compliant manner. However, because the

TABLE 5
Data Protection Officer and Data Protection Representative

- Data protection officer (DPO):
  - Framework setup
  - Accountability documentation
  - Oversight on behalf of the sponsor
  - Risk assessment and management
  - Inform, advise, and monitor
- Data protection representative (DPR):
  - Required by organizations established outside the European Economic Area
  - Point of contact for data subjects and authorities
  - Appointment of representative is irrespective of adequacy
  - Must be established in a relevant Member State
  - Post-Brexit, both E.U. and U.K. GDPR Article 27 apply:
    - Two representatives are required

CRO is a data processor and not a data controller, they will not be subject to the same data controller requirements as the sponsor. The data protection officer is there to bridge this gap, provide the necessary oversight, and enable the sponsor, as the data controller, to demonstrate accountability for the personal data processed.

A CRO, however, is just one of the many data processors involved in a clinical trial. The sponsor must assess each data processor for risk to ensure they too will apply appropriate technical and organizational measures to protect the data. A specific data processing agreement needs to be implemented to govern the contractual terms for the data processing. These are all specialist tasks the data protection officer is well placed to handle on the sponsor's behalf.

A data protection representative (DPR) is a requirement for organizations based outside the European Economic Area that have no physical establishment within the area. This applies to many global life sciences organizations that are located outside of the European Economic Area and conduct clinical trials within the E.U. and the U.K. The role of the data protection representative is to act as a point of contact for E.U. data subjects and authorities. Even if the sponsor is based in a country the European Commission deems to be adequate, such as Japan, New Zealand, and South Korea, appointment of a DPR is necessary.

Some CROs do provide data protection representative services, however, they may lack the necessary expertise when dealing with regulatory inquiries. Most importantly, CROs are unlikely to be able to avoid a conflict of interest should they ever need to deal with a data breach, especially if they are responsible for the breach.

The U.K. GDPR, which became effective on January 1, 2021, is currently essentially the same as the E.U. GDPR. This means that sponsors conducting clinical trials in one or more of the 27 E.U. Member States and the U.K. must comply with two GDPRs. Therefore, it is necessary to appoint a data protection representative in both the E.U. and the U.K. In the proposed Data Protection and Digital Information Bill (No. 2) which is currently being considered by U.K. Parliament, the U.K. is proposing to remove the requirement to appoint a U.K. data protection representative. Informed consent forms, privacy notices, the CNIL MR-001 self-declaration, and the standard

contractual clauses all now require the identification of E.U. and U.K. data protection representatives.

Key Steps to Consider

When processing E.U. and U.K. personal data, first and foremost, sponsors must understand their data flows, cross-border transfers, lawful bases, and processing risks. Sponsors must implement an E.U. GDPR compliance framework prior to enrolling the first participant in a clinical trial.

Also, sponsors must ensure they clearly map their data and identify each of the third party organisations involved in the trial's data flow. Sponsors must determine whether the third party resides in a third country and if so, determine whether that third country is subject to other regulations such as the US's FISA Section 702.

Where necessary, the sponsor must ensure any standard contractual clauses (SCCs) used are accompanied by a transfer impact assessment (TIA). Regardless of the location of the third parties receiving the clinical trial data, the sponsor must demonstrate that it has conducted adequate due diligence to ensure it has met its obligations to appoint only appropriate data processors to maintain the standards expected under the E.U. GDPR.

If not already completed, and where relevant, the sponsor must conduct a data protection impact assessment (DPIA). This assessment helps the sponsor understand the risks associated with data processing for the clinical trial, especially any risks involving sensitive special category data.

Sponsors must also amend their data breach procedures, escalation pathways, and notification protocols. Under the E.U. GDPR, the data controller has only 72 hours from the point of becoming aware of a data breach to notify the relevant authority.

Also, sponsors must ensure they have implemented data processing agreements with all relevant study partners and clinical research sites throughout the data processing chain. Data processing agreements are legally binding documents between the data controller and each data processor. These agreements regulate the scope and purpose of the data processing, as well as the relationship between the data controller and the data processer.

Data processing agreements ensure both parties understand their responsibilities. Also, they define what a data processor can and cannot do in processing personal data. The data processors are, in turn, required to implement data processing agreements with their sub-data processors. Ultimately, however, the data controller is responsible for ensuring data processors have implemented data processing agreements with third parties for any onward transfers.

Sponsors must update their Records of Processing Activities (RoPA) and identify the data transfer mechanism used for cross-border data transfers. If a data protection representative (DPR) is required, as a minimum, the sponsor must provide the representative with a copy of the RoPA.

Also, sponsors should become familiar with the requirements of the CTIS. Since January 1, 2023, all E.U. clinical trial applications have to be submitted using the system. Starting January 1, 2025, any clinical trials implemented under the previous E.U. directive must be migrated over to the CTIS.

Sponsors must determine whether they are required to appoint a data protection officer (DPO) and/or a data protection representative (DPR). In most clinical trials, it will be necessary to appoint both. The DPR is essentially a passive and reactive role. The purpose of the DPR is to be available to respond to questions and requests as they arise from E.U. and U.K. data subjects and regulators. Having a DPR enables data subjects to avoid the inconvenience of contacting a data controller who may not speak their language and who may be based in a different time zone.

The DPO is much more proactive. As defined by the E.U. GDPR, the role of the data protection officer is to inform, advise, and monitor compliance of the data processing activities. In the pre-trial phase with clinical trial sponsors, however, it is common for the

DPO to be much more hands-on. This includes providing support in drafting policies, defining procedures, liaising, and negotiating with vendors and partners, conducting risk assessments, and actively and proactively mitigating those risks.

Appointing a DPO based in the E.U. supports sponsors in complying with the requirements of the E.U. GDPR and the Clinical Trials Regulation. Also, data protection officers in the E.U. have the appropriate skills and experience to protect the sponsor's interests as the data controller and to provide appropriate oversight of the activities of data processors. Both the DPO and the DPR can be easily outsourced. It is imperative, however, to select a provider who has detailed knowledge of and experience in the requirements of running clinical trials within the E.U.

SELF STUDY ANSWER KEY

FDA - Guidance for Industry
Circumstances that Constitute Delaying, Denying, Limiting, or Refusing a Drug or Device Inspection
Draft Guidance
Part 2

ANSWERS

1. d. all the above (Section V)
2. b. False (Section V Part B)
3. d. 702 (Section V Part D)
4. a. deny (Section IV)
5. c. A facility provides the FDA investigator the requested records that FDA has authority to inspect, but they are reasonably redacted. (Section V Part C)
6. b. False (Section V Part C Footnote #1)
7. a. Without an unreasonable explanation, the facility bars the FDA investigator from entering the facility. (Section VI)
8. a. A facility accepts FDA's attempt to schedule a pre-announced inspection. (Section IV)
9. e. All the above. (Section V Part B)
10. a. True (Section VI)