European Union General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR) goes into effect May 25, 2018, replacing the existing EU Data Protection Directive. While the regulation is intended to cover EU personal data, non-EU entities may still be impacted by the new requirements.

Note: If you are unsure whether the GDPR applies to your particular study or scenario, we suggest consulting with research compliance for guidance.

What Is the GDPR?

The General Data Protection Regulation (GDPR) establishes and enhances protections for the privacy and security of personal data about individuals within the EU. It places restrictions on handling personal data and delineates the responsibilities and obligations of companies processing personal data.

GDPR Terminology:

•Data Controller: The person or legal entity responsible for determining the purpose and means of processing personal data.

- For clinical trials, this is the sponsor. Another entity may be considered a joint controller (e.g., a CRO or investigator in an academic clinical trial).

•Data Processor: The person or entity who processes personal data for the sponsor.

•Data Subject: The individual(s) within the EU who are having their personal data collected and processed.

•Data Protection Officer (DPO): The person responsible for overseeing data protection strategy and implementation in compliance with the GDPR requirements.

•Identified Person: Someone who can be identified, directly or indirectly, through the following identifiers: name; an identification number; location data; online identifier; or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

What Does the GDPR Cover?

The personal data categories covered under the GDPR are broader than protected health information covered by HIPAA or identifiable private information included in the Common Rule. Under the GDPR, personal data is "any information relating to an identified or identifiable natural person" (AKA the "data subject"). Even coded data (or "pseudonymized data") is considered personal data that would be subject to the protections of the GDPR. Data that have been fully anonymized are not covered by the GDPR.

The GDPR further defines special categories of data, called "sensitive personal data," which are subject to stricter regulation. This would include data typically collected in a clinical trial, including health data, genetic data and biometric data. This category also includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation.

How Does the GDPR Apply to Clinical Research in the EU and Beyond?

The GDPR is intended to cover EU personal data, including data processed for clinical trials and applies directly to companies located in the EU, Iceland, Liechtenstein and Norway. It also applies to the processing of personal data by a controller or processor not located in the EU when the data processing is related to (a) offering goods or services to participants in the EU, or (b) the monitoring of behavior of participants while in the EU.

It applies to anyone while in the EU, not just EU residents. This means that the GDPR may affect US clinical trials even if the trial is not conducted in the EU.

Example: *A US citizen enrolls in a clinical trial in the US that requires her to wear a device that collects her health information. She travels to the EU while participating in that study and continues to wear her device, which continues to collect her health information. All personal data collected and transferred to the US while that participant is in the EU is subject to the GDPR.*

On the other side of the coin, the GDPR generally will not apply to EU citizens enrolling in a US clinical trial while located in the US. However, if the clinical trial is being advertised in the EU, or if participants are followed or follow-up care is provided when participants return to the EU, then the GDPR may apply.

How Are Study Participants Informed of GDPR Data Privacy Requirements?

The clinical trial sponsor is responsible for determining whether the study must comply with the GDPR. If the study is subject to the GDPR, detailed data privacy information must be provided to participants. This data privacy notice may be included in the informed consent form, a data privacy addendum, a letter to participants, or other formats as determined by the sponsor.

The IRB should confirm that the GDPR data privacy requirements have been included in the data privacy notice. Some of these elements are already included in typical clinical trial consent form templates. The additional elements related to data privacy that must be included in the data privacy notice include:

•Identity and the contact information for the sponsor (AKA the data controller).

•Contact information for the data protection officer (if there is one).

•Special categories of personal data that will be collected for the study, such as:

- Age, sex, ethnic and racial background.
- Health and medical conditions including past medical history.
- Study procedures and response to procedures.
- Information related to the participant's sex life.
- Biological samples (e.g. urine, blood, tissue and the results learned from analyzing them).
- Medical images (e.g. ultrasound scans) and the results learned from evaluating them.

•Data privacy rights:

- The right to request information about the handling of the participant's data. ***Note:*** *It is acceptable to add a limitation that, for scientific integrity, access to some of the data may not be allowed until the study ends.*
- The right to request correction of data if it is inaccurate or incomplete, and to restrict processing while it is being corrected.
- The right to request transfer of data to the participant or others in a commonly used format.
- The right to withdraw consent at any time, including the right to withdraw from study participation, follow-up or further handling of data. ***Note:*** *It is acceptable to add a limitation that data already processed is legally covered by the original consent, but no further data will be collected.*
- The right to request deletion of the participant's data if the data are no longer needed, or there is no other legal requirement for their use. ***Note:*** *FDA regulations require retention of the participant data for specified periods of time.*

- The right to file a complaint with a data protection authority.

- The right to know the recipients or categories of recipients of the personal data, if any, and the identity of the people who may have access to the data. ***Note:*** *This is usually already covered in the HIPAA authorization.*

•Transfer of data (if data will be transferred to others): A statement about the circumstances under which it will be transferred and safety measures taken to protect the data (e.g., data are encoded). If this is already described in the main ICF, the data privacy notice may simply reference the ICF (e.g., "as described in the consent form").

- If data will be transferred outside the EU: A statement that the countries who are receiving the data may not have had their data protection level confirmed as adequate by the European Commission, and any safety measures taken to protect data privacy rights. ***Note:*** *The EU has not confirmed that the US has an adequate data protection level.*

•Retention of data: A statement describing how long data will be stored.

How should consent be obtained?

The GDPR does not require signed written consent for data processing, even for the processing of special categories of data typically collected in a clinical trial. The study sponsor (as the data controller) must be able to demonstrate that valid explicit consent was obtained. Although written consent via the main informed consent form or a consent addendum would be considered best practice, oral consent is sufficient.

Reconsent is not required for the use of data collected prior to May 25, 2018, provided that the way consent was previously given is in line with the conditions of the GDPR. The will depend on whether older consents meet the requirements for consent under the GDPR: freely given; informed; specific; unambiguous by a clear statement or affirmative action of consent (e.g., signing the consent form). Older consents meeting these requirements are likely to be considered valid, even though the data privacy notification was not originally included.