PHARMA HORIZON PHARMA HORIZON PHARMA HORIZON **PHARMA HORIZON**

PRIVACY COMPLIANCE AND CLINICAL TRIALS

Keywords: Clinical research, privacy, health data, accountability, data security, data quality.

Sophie Bernard *(Privacy & Data Protection Manager, PRINEOS srl) has grown a solid experience in the field of data protection in healthcare and contract research industries and defends that understanding the rules applicable to clinical research is essential to find the right balance between scientific progress and protection of patients' rights and freedoms.*
PRINEOS srl is a new strategic consulting company born and raised by passion, leveraging on a team with more than 25 years of expertise in the Life Sciences.
Our goal is to improve and innovate Clinical Research in Healthcare providing services on: Biostatistics, Medical Affairs, Regulatory and Legal Affairs.

Sophie Bernard
PRINEOS srl, Milano, Italy

INTRODUCTION

Clinical trials are challenging by definition. Even though any clinical research entails a certain degree of uncertainty regarding its potential success, several clinical trials challenges come with opportunities for improvement and are major drivers of innovation.

PRINEOS srl proposes this column with the aim of spreading greater awareness about challenges and opportunities for improvement in clinical trials, addressing several crucial topics in this context.
Our journey starts with the topic "Privacy Compliance and Clinical trials" as privacy compliance has been (and may still be) quite challenging for all stakeholders involved in clinical research, considering also the lack of a general legal framework on this subject.

In the upcoming articles we will cover key aspects of clinical research methodology being critical for the success of a clinical trial, namely the sample size calculation and the endpoints definition. As highlighted by a research from the Tufts Center for the Study of Drug Development, nearly 60% of clinical study protocol require at least one substantial amendment with an average cost per amendment of $453,932. Most notably, 34% of all amendments were avoidable, as due to protocol design flaws, such as inappropriate primary endpoint or sample size, or recruitment difficulties.

Afterwards, we will discuss modern concepts in clinical research that are challenging and changing the traditional trial paradigm and landscape: decentralized (or virtual) and Real Word Evidence (RWE) clinical trials.

Finally, we will address the growing complexity of the regulatory framework for clinical trials: are we going to be able to meet the needs of an increasingly complicate landscape while maintaining effectiveness and efficiency?

With these series of articles our main purpose is to turn issues into opportunities: each challenge may become a chance to redefine processes, methods and procedures, as well as a major driver for improvement.

One of the main challenges in clinical research is related to study data management and patients' privacy protection (1).

Data Privacy impacts all clinical study projects, from the project design phase, throughout the trial's execution and until its conclusion. This article explains how to ensure compliance with the main privacy-related requirements applicable to the entire clinical study life.

DURING THE INITIAL TRIAL STAGE

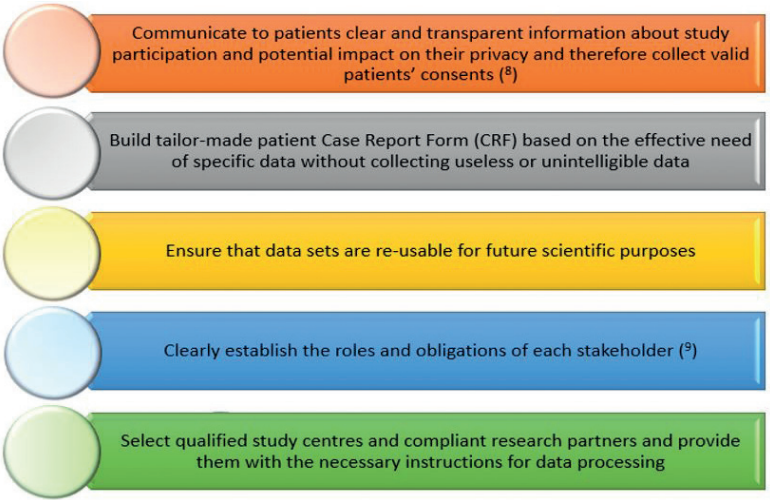
Before a clinical trial may even start, extra care shall be dedicated to personal data protection.

Clinical trial stakeholders must learn how to demystify data protection principles (2), as the "Privacy by design/by default" principles (3) according to which data controllers (4) must aim at personal data protection, by default, while defining procedures for data management, and by design, as soon as a processing operation is contemplated and, in any case, before any data is collected or accessed.

For instance, when planning for a study project, researchers must define *a priori* some elements as for example subjects' inclusion criteria, sample size, select study sites, etc. At this point, study sponsors must also, among other things, determine the purposes and means of data processing operations, set up categories and number of data records necessary for the trial, prepare study documentation and initiate approval process with the competent review board/ethics committee, and determine who will access the data, etc. When doing so, the following principles shall be carefully applied:

- **Lawfulness and transparency** of the processing operations (5) – Are all research stakeholders authorized to process patient study data lawfully? Have trial participants been informed about the processing of their data?
- **Purpose limitation** (6) – Will patient study data include data collected as part of another study protocol? Did the primary consent form contemplate secondary scientific purpose(s)?
- **Accountability** (7) – Did you define the roles and responsibilities of all stakeholders involved in the trial's execution? Did you sign a written agreement with all processors and ensure they implemented appropriate data privacy and security safeguards for patient study data management?

Compliance with those privacy principles can be used to create a privacy checklist for the study planning phase that could include the following achievements:



WHEN THE TRIAL IS ON-GOING

At this point, data collection goes on smoothly and data sets are getting bigger. Study researchers must now be able to demonstrate and guarantee data integrity, quality and security.

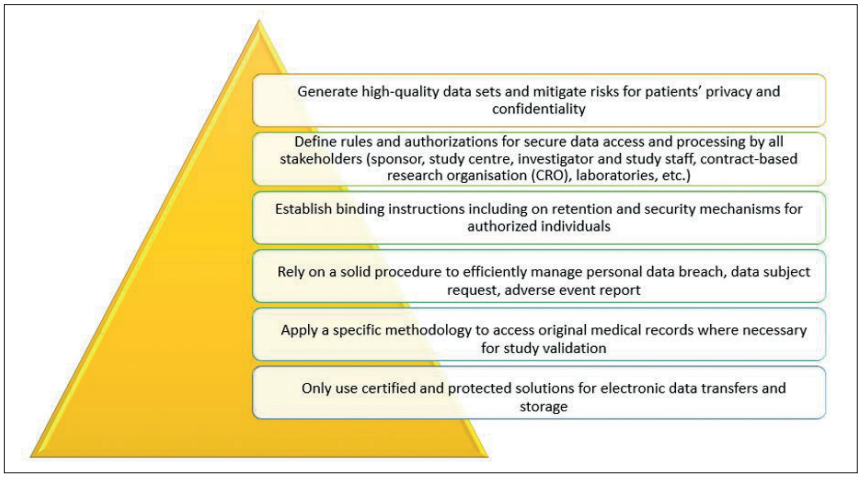
Given the highly sensitive nature of the data processed during clinical trials (i.e., data concerning health, genetic and/or biometric data (10)), data protection authorities require clinical study organisations to implement specific technical measures to enhance patients' confidentiality and data security, to prevent accidental or unlawful modification, loss or destruction and unauthorized access (potentially resulting in a personal data breach (11)).

International legal and regulatory frameworks on clinical trials recommend encoding patients' data to avoid individual's re-identification by combining patient study data with additional information, whether by using de-identification (12), pseudonymisation (e.g., data associated with a unique alpha/numeric code – so-called "patient ID") or anonymisation (13) techniques. For example, the Italian Data Protection Authority ("Garante") advises (14) making the data anonymous in all circumstances in which this operation is feasible. When neither anonymization, nor pseudonymisation is achievable because access to original medical records is necessary (e.g., for Source Data Verification (15) (SDV) performed by in-house or third-party clinical research associates), clinical study organisations must implement additional safeguards to ensure patients' confidentiality and data integrity.

More specifically, here are the data protection principles to be contemplated:

- Data minimization (16) and accuracy – Are encoded data sets intelligible? Did you collect high-quality and accurate data?
- Integrity and confidentiality (17) – Do you have user authentication and access control process? Did you and your partners implement secured channels to share and store patient study data?

Building a data management strategy based on such principles would allow clinical study organisations to:



AT THE TRIAL'S CONCLUSION

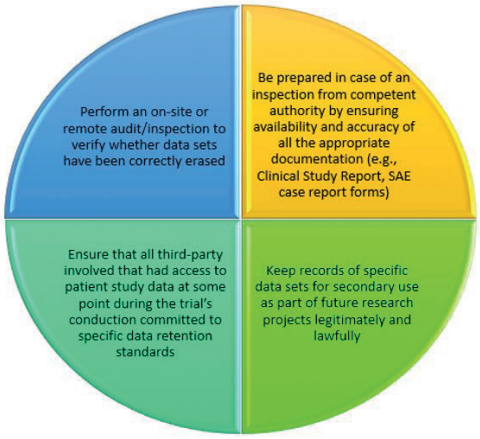
Unfortunately, data privacy concerns do not vanish at the end of the clinical trial. On the contrary, at this stage, study sponsors shall ask themselves what to do with all data sets gathered as part of the study.

According to the EU and national data protection laws (18), data controllers may retain personal data only for as long as is necessary to achieve the defined purposes. In other words, as soon as data are no longer helpful for the clinical trial's execution, study sponsors shall promptly anonymize or permanently erase all patient study data from their database, as well as from those of their third-party suppliers (e.g., cloud service provider, patient transport service provider, study laboratory and depot).

When some data shall be kept for legitimate reasons (e.g., compliance with a legal requirement including pharmacovigilance obligations, re-use of patient study data outside the scope of the primary protocol for another scientific purpose (19)), if patients are not informed about this possibility in the primary consent form or information notice, data controllers might need to get another specific consent or, at least, provide a complete information notice to data subjects.

- **Purpose and data storage limitation** (20) – How long can you keep the data? Should you anonymise or delete the remaining data sets? How to ensure data security and confidentiality for data that must be kept as per legal or regulatory requirements?
- **Accountability** – Did all stakeholders receive clear instructions for data deletion/ restitution at the end of the study? Do you have a right to audit your processor's IT infrastructures and facilities to verify data quality and security?

Keeping in mind such data protection principles would allow clinical research organisations to:



CONCLUSION

Although compliance with data protection standards requires deep knowledge and understanding, clinical study organisations shall seize the opportunity to invest in privacy matters in order to establish truthful and transparent relationships between researchers and trial participants, ultimately, to improve patients' experience, but also to facilitate and guarantee data quality, accessibility and integrity for reliable and pertinent study results.

REFERENCES AND NOTES

1. see also the European University Institute guide on good data protection practice in research of 2021.
2. see GDPR art. 5
3. see GDPR art. 25
4. see GDPR art. 4, § 7
5. see GDPR art. 5, § 1, let. a) – see also the European Data Protection Board (EDPB) Opinion n. 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR), adopted on 23 January 2019
6. see GDPR art. 5, § 1, let. b)
7. see GDPR art. 5, § 2
8. In particular, see the EDPB Guidelines n. 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020
9. see the EDPB Guidelines n. 07/2020 on the concepts of controller and processor in the GDPR, adopted on 02 September 2020, in particular, see examples for clinical trials on pages 21-22
10. see GDPR art. 4, § 13 to 15 and art. 9
11. see GDPR art. 4, § 12
12. see the US Health Insurance Portability and Accountability Act (HIPAA) of 1996 for de-identification of "Personally Identifiable Information" and "Protected Health Information" (PII/PHI) (Public Law 104-191)
13. In particular, see section 6 of the EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 February 2021
14. Specifically, see the Italian Garante "Guidelines for the processing of personal data in the context of clinical trials of medicines" published on 24 July 2008
15. In particular, see the ALCOA-C standards for clinical trial electronic document management in accordance with the Good Clinical Practices (GCP)
16. see GDPR art. 5, § 1, let. c)
17. see GDPR art. 5, § 1, let. f)
18. Mainly Regulation (EU) 2016/679 on personal data protection (GDPR) of 27 April 2016 and all local privacy laws issued following its entry into force
19. see also art. 28 of Regulation (EU) 2014/536 on clinical trials (CTR) of 16 April 2014
20. see GDPR art. 5, § 1, let. e).