Recommendations for General Data Protections Regulation (GDPR) Compliancy by the PHUSE Data Transparency Working Group

Arlene Coleman, Pfizer, USA
Shannon Labout, Data Science Solutions LLC, USA

ABSTRACT

The PhUSE Data Transparency Working Group GDPR Project team is writing a white paper with recommendations for applying GDPR rules to data clinical research studies. This paper has been prepared by the GDPR Project sub-team leads with the intent to list and discuss the research process and recommendations that will be summarized in the PhUSE GDPR White Paper.

INTRODUCTION

The General Data Protections Regulation (GDPR) from the European Parliament was published in 2016 and became enforceable in 2018, standardizing data privacy laws across Europe. GDPR's purpose is to ensure privacy and security of personal data collected in the process of any business operation, including clinical research. GDPR grants significant new rights to citizens of European countries, including the right to be forgotten, as well as promoting transparency on how patient data is collected and used. The interpretation and application of the regulation in clinical research has been an important topic of conversation. PHUSE convened a GDPR data transparency working group project in 2018 to research and discuss GDPR compliancy, focusing on completion of a White Paper in 2020. This paper will summarize some findings of the GDPR Project based on PHUSE working group internal research as well as recommendations collected from survey results.

GDPR includes some exemptions for special categories of data, of which clinical research data is one. This does not mean that clinical research data would be exempt from all provisions of GDPR, but certain provisions (such as the right to erasure) would not apply. A discussion of those exemptions as well as informed consent is outside the scope of this paper.

PHUSE GDPR PROJECT

The PHUSE Data Transparency Working Group has worked on several projects, including developing a Data De-Identification Standard for SDTM and creating a Data Transparency Roadmap. In 2018 the Data Transparency Working Group started a project to address the impact of GDPR on clinical research data collection practices. The GDPR Project is composed of multiple sub-teams who joined together for the purpose of sharing experiences, approaches, recommendations and understanding of GDPR compliance:

DATA COLLECTION AND PERSONALLY IDENTIFYING INFORMATION (PII)
Data collection activities for GDPR alignment and compliance, including how to handle the collection of PII such as birth date or age across age ranges and study types, and what to collect or not collect for different study types.

DATA BREACH, SAFEGUARD AND PROCESSES
GDPR requirement implications surrounding data sharing and data breach recommendations, long-term approach of archiving and storing data, other country regulations specific to GDPR, communication between sponsors and CRO's, data retention periods, data anonymization and database access. Overall process, documentation and communication specific to protecting patient data privacy is considered.

The GDPR White Paper has been publicly reviewed and in the process of finalizing before being officially published in 2020.

DATA COLLECTION TOPICS

The Data Collection and PII sub team focused on developing working definitions for terms that would be used in the White Paper, identifying commonly collected data points that could potentially be PII, and discussing the handling of these data points. As part of the process, this team researched the impact of GDPR on data collection activities by reading the GDPR documentation, and through informal public surveys shared through LinkedIn and by email. Information collected included:

1. Identifying information that would be considered personal data, and has the potential to trace back to an individual research participant
2. Researching current practices and recommendations for minimizing the collection of personal data and mitigating the risks associated with collecting that data
3. Identifying opportunities to align data collection practices with GDPR

The completed public survey specific to these topics included recommendations from 30 respondents across multiple pharmaceutical, biotechnology and CRO companies. Interesting survey conclusions and recommendations revealed that most companies are limiting the collection of Birth Date and Age to what they need for a particular study population and analysis. For example, if they were conducting a study in which Centers for Disease Control (CDC) growth charts were being used, they were required to collect an exact birth date to use the growth chart effectively. However, for most non-pediatric patient populations, Birth Year or Age were sufficient to apply lab ranges and other age-related factors. Keeping in mind that there may be regional restrictions on what is appropriate to collect.

Recommendations approaching the collection of Birth Date / Age are as follows:

- Collect the minimum amount of information needed to achieve study analysis needs
- Ensure to follow regional privacy rules in which the study will be conducted
- Studies involving adult populations, Age (or year of birth only) is sufficient
- For pediatric populations, consider the following:
    - What collected data is actually required for the study
    - Age group (may be different for very young infants vs. teenagers)
    - Therapeutic area (e.g., growth studies may have more precise requirements)
    - ICH requirements to track pediatric patients against growth charts
- For most pediatric studies (if there are no other factors)
    - Up to 2 years old, collect full Birth Date
    - From 2 years to 18 years, collect Month and Year
- Pediatrics is typically considered to be up to 18 years. This may differ by region
- Recommendations for Birth Date precision may differ by data source/collection method. Additionally, data needed to reconcile across data sources may drive what is needed for collection. Additional examples to consider will be summarized in the final GDPR White Paper

DATA BREACH, SAFEGUARD AND PROCESSES SURVEY AND RECOMMENDATIONS

As described above, many topics were discussed surrounding safeguarding patient study data, specifically to ensure GDPR compliancy. After internal review and a completed survey to obtain recommendations from PhUSE members and cross industry participants, the working group summarized valuable information including the following:

ACCESS RESTRICTIONS

- Access to files that contain participants' Personal Data should be limited to the designated study team members. If additional staff members outside of the clinical study team require access to the clinical data, this can be provided once reviewed and approved by appropriate designated approvers
- It is suggested to allow access to only a subset of data (if applicable to the needs) and renew clinical study data access on a periodic basis
- Informed consent and Primary/Secondary analysis definitions within the study protocol require review to ensure participants have agreed to how their data can be used, including for any purposes beyond the original study such as pooled analyses
- Anonymization of data is required if data may be shared more widely in a secure fashion, depending on the research activities and appropriate approval process

SAFEGUARDING OF DATA

- Proper IT security assessments, specifically when sharing data with a CRO (Contracted Research Organization) should be conducted. Sponsors expect CRO's to have robust network security procedures, firewalls, issue resolution protocols, and an auditable record of data accessors
- An agreement of contract was an agreed upon essential method of safeguarding data based on survey results. The agreement introduces data safeguarding obligations. The contract is also the foundation upon which the Sponsor/CRO relationship is built.
- Manual of Operations and training recommended for data safeguarding awareness
- Sponsor review of CRO's training requirements and SOPs
- Storage and archive of final documents and reports should be considered
- Periodic checks to ensure company specific policies are being followed
- Permanent data storage should be at sponsor only
- It is a high risk to discuss or share data via email

- Establish formal data management and access process or procedures to minimize sharing of or unauthorized access to Personal data
- Follow secure data transfer modalities
- Follow proper anonymization methods and risk assessments before sharing data externally for external data researchers

DATA BREACH

- Take effective preventative measures by providing GDPR specific training for personnel CRO's to ensure standard operating procedures are being followed. Include how to address accidental breaches such as CAPA and preventative/corrective measures for GDPR audit readiness
- Periodically verify that personnel are up to date with training, test IT systems for security, ensure systems have robust data audit trails, conduct awareness training on a regular basis, conduct workshops to make the situation 'real' to all employees, make SOPs user-friendly, and avoid recording / maintaining / sharing personal data (unless data is anonymized and approved to share). An organization should have a standing data security/data privacy policy in place that outlines the steps to limit and safeguard data.

In all, 23 people responded to this survey, ranging from pharmaceutical/Sponsor companies and CROs. The results were largely free text, which will be further summarized in the GDPR White Paper.

CONCLUSION

Recommendations proposed by the Data Transparency Working Group based on internal research and survey results include following all current laws and predicate rules that govern data integrity and provenance.
Limit collection of data to necessary data only, reducing to only collecting data necessary for the analysis. Ensure informed consent clarifies how collected data will be used, protecting patient privacy at all times. Take preventative measures and actions to safeguard and protect clinical research data. A White Paper is currently being finalized by the Data Transparency Working Group. Once agreed as final, the White Paper will be published and made available through PHUSE in 2020.

Disclaimer:

This is an interpretation of GDPR with suggestions for possible ways to apply it in practice based on opinions from individuals in PhUSE working groups and unidentified survey respondents. It does not constitute legal advice.

REFERENCES

GDPR Website:
https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

PhUSE Data Transparency Working Group Wiki:
https://www.phusewiki.org/wiki/index.php?title=Data_Transparency

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:
Author Name: Arlene Coleman
Company: Pfizer
Work Phone: 862-324-1036
Email: arlene.coleman@pfizer.com

Author Name: Shannon Labout
Company: Data Science Solutions LLC
Address: 223 Salt Lick Road, Suite 279
City / Postcode: St. Peters, MO 63376
Work Phone: 917-821-7165
Email: Shannon.Labout@DataScienceSolutionsLLC.com
Web: www.DataScienceSolutionsLLC.com