AMERICAN MEDICAL WRITERS ASSOCIATION AMWA JOURNAL V39 N3 / 2024

REGULATORY INSIGHTS

European Union Regulation on Personal Data Protection in Medical Writing

Tatiana Revenco, PhD / Privacy Professional and Personal Development Lead, MyData-TRUST, Mons, Belgium

ABSTRACT

The European General Data Protection Regulation 2016/679 (GDPR) aims to harmonize data protection laws across European Union (EU) Member States. The goal of GDPR is to ensure respect of the fundamental right to protection of the personal data and privacy, to enhance security measures, including information technology (IT) for data protection, and to render natural persons control over their personal data. Importantly, companies, institutions, freelancers (including medical writers) located outside the EU and handling personal data of natural persons living on the territory of the EU must comply with GDPR.

Medical writers edit documents related to the activities in health sector that comprise personal data, specifically health data considered as sensitive data. Therefore, medical writing should put in place robust security measures and comply with the GDPR. This article is a clarification of the GDPR notions, principles, technical and organizational measures applied to the medical writing to guarantee protection of the personal data and respect of individual's rights and freedoms.

INTRODUCTION

The European Union (EU), consisting of 27 European member states (MS),[1] is governed by the European Parliament and the Council of the European Union. These two legislative bodies, comprised of EU MS representatives, are responsible for enacting legislations (that comprise regulations and binding legislative acts) that apply across all MS. The European General Data Protection Regulation 2016/679 (GDPR) was voted by the European Parliament and the Council of the European Union as a binding regulation for all EU MS, aiming to harmonize the national data protection laws of all EU MSs.[2,3]

The GDPR respects all fundamental rights and observes the freedoms and principles recognized in the Charter of Fundamental Rights of the European Union and in the Treaty on the Functioning of the European Union. The objective of the GDPR is acknowledging the right to protect personal data (PD) and respect individuals' privacy, freedom of thought, conscience, and religion, freedom of expression and information, as well as freedom to conduct a business. In addition, the GDPR aims to enhance security measures by leveraging information technology (IT) to protect PD and to render individuals' control over their own PD. In principle, companies, institutions and freelancers, including non-EU medical writers and those handling PD for EU residents, should comply with the GDPR. Medical writers usually edit the health system documents that contain sensitive PD. Thus, medical writing should employ robust protection of PD as required by the GDPR. This article clarifies GDPR notions, principles, and technical measures applied to medical writing to support PD protection and respect of the aforementioned individuals' rights and freedoms.

GDPR NOTIONS ASSOCIATED WITH MEDICAL WRITING

Requirements for the Management of Sensitive Data

PD are defined as any information related to a natural person. The person can be directly indentifiable by name, surname, identification number, or other direct identifiers. Or the person can be indentified indirectly by combining other personal information or factors such as physical, physiological, genetic, mental, cultural, and so on.[3]

When editing documents representing a particular clinical study, medical writers may manage PD, including demographic information (ie, age, gender, ethnicity, and race), health and genetic data, which is classified as sensitive PD.[3] Sensitive PD falls under special categories of data and requires enhanced security measures with a comprehensive and multiple-faceted strategy.

Complying With GDPR When Processing PD

The GDPR defines actors of processing activities. A data controller is a natural or legal person, public authority, agency, or other body that, alone or jointly with partners, determines the purposes and means for processing PD. In the context of a clinical study, controllers are the sponsor or

ISSN 2163-5315

investigational site; they determine the objectives and means of processing the study participant's data in the study protocol. The GDPR clearly defines the duties and liability of the controllers. As such, controllers should implement appropriate and efficient security measures to demonstrate compliance with the GDPR in processing activities.

Data controllers engage service providers or freelancers, including medical writers, who are defined as data processors. Although processors handle PD upon the instructions of controllers, they have responsibilities and obligations to provide sufficient guarantees to implement appropriate security measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the data subject's rights.[1] The contractual bindings between controllers and processors must incorporate a data processing agreement (DPA) that explicitly outlines the responsibilities of both parties and ensures compliance with the GDPR (Figure 1).

GDPR PRINCIPLES APPLIED TO MEDICAL WRITING

The GDPR outlines key principles that serve as the foundation for data protection. These principles guide how organizations process PD.

Lawfulness, Fairness, and Transparency

The GDPR states that PD shall be processed lawfully, fairly, and transparently in relation to the data subjects.[3] Accordingly, the processing of PD must have a valid legal basis, such as the consent of data subjects, the legitimate interest of controllers, or a legal or contractual obligation. Fairness is defined as the idea that PD processing should not exceed data subjects' expectations. Transparency means that the purposes and means of processing must be clearly defined and explained in a comprehensible language to the data subjects (ie, informed consent forms for a clinical trial, plain language sections in the articles or patient advocacy communication, privacy notices for digital communication or any other types of communication).

Purpose Limitation

The GDPR restricts the collection of PD to specific and explicit purposes initially disclosed to the data subjects. It prohibits using PD in ways that are incompatible with those stated purposes. However, if a second purpose arises, it must undergo a thorough analysis to determine its compatibility with the initial purpose. If it is not compatible, additional steps for data re-use are necessary. However, further details on this topic are beyond the scope of this article.

Minimization

The GDPR states that "PD shall be adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed."[3] When writing for scientific publications, data minimization means that any additional information about an individual must be avoided or replaced with more generalized information.[4-7] Examples of generalization or randomization of PD include: avoiding the use of date of birth, using a range of age to replace exact age, removing any unnecessary details on images (ie, from scans, biopsies, x-rays), double coding a patient code that was initially attributed by the investigational site, avoiding or generalizing (by a considerable geographical extent) the location and name of the investigational site, and removing or aggregating outliers.

Accuracy

The GDPR specifies that PD must be both accurate and, when necessary, kept up to date. Moreover, the regulation emphasizes that every reasonable effort should be made to promptly erase or rectify inaccurate PD, considering the purposes for which they are processed. Overall, a particular set of PD should be attributable, legible, contemporaneous, objective, and accurate. The accuracy of data is ensured by additional teams that perform quality control, and the correctness of data is used to do statistical analysis, elaborate figures, and create tables for any medical documentation, report, or publication.

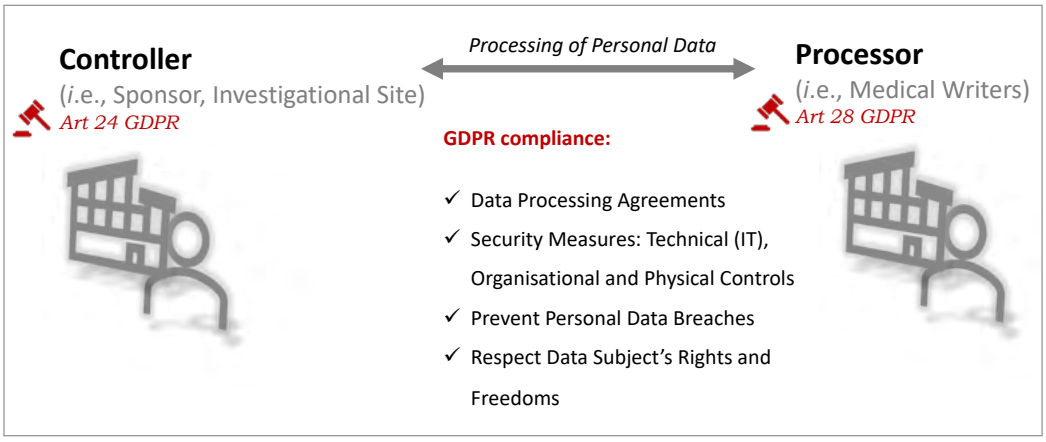

Figure 1. Responsibilities of data controllers and processors. GDPR, European General Data Protection Regulation 2016/679.

Limitations on PD Retention

The GDPR does not prescribe specific retention periods; it mandates that data are stored only as long as necessary in accordance with relevant regulatory provisions and the specific purposes of data processing. Organizations must therefore develop and adhere to a robust data retention policy tailored to their sector and operational needs. For instance, in clinical research, the storage duration of data depends on the type of investigational product and the relevant regulations. Clinical Trials Regulation apply when the investigational product is a drug, requiring data to be stored for at least 25 years, whereas the PD holding span for advanced therapy medical products is 30 years.[8,9] On the other hand, as per medical device regulation, the estimated PD lifespan for clinical studies on performance evaluation of medical devices, including health applications, falls between 10 and 15 years.[10] Without regulatory specifications, controllers should follow the commendable retention duration for a set of PDs from regulatory authorities. Otherwise, the controller may define the retention time by relying on the processing objectives.

Notably, the data controller is responsible for instructing processors on the duration of retention, retrieval, and deletion of PD upon termination of the data lifespan. In most cases, the storage period is limited to the provision of services mentioned in the contracts; otherwise, data protection agreements should address the data holding period.

APPLYING MEASURES TO PROTECT PD

Data controllers and processors must put security measures in place and ensure privacy by design and default.[3] The goal of security measures is to prevent PD breaches and decrease the risks of threats to the rights and freedoms of data subjects. Security measures defined by the GDPR include

- the pseudonymization and encryption of PD;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
- the ability to restore the availability and access to PD on time in the event of a physical or technical incident; and
- a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Importantly, the GDPR doesn't impose either pseudonymization techniques or any other technical and IT specificities (ie, algorithms for encryptions, types of encryptions), rendering the possibility for controllers and processors to adopt the measures according to their type of processing activities, size, organization, and budget.

> *Pseudonymization is the processing of PD in such a manner that the PD can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the PD are not attributed to an identified or identifiable natural person.*[3]

Investigational sites attribute a code instead of their names to avoid direct identification of study participants in clinical trials. The codes remain confidential by the sites, and the data controller (sponsor) and processors (service providers) do not have access to the key to the code. Thus, they handle pseudonymized data of study participants. Other pseudonymization techniques in medical writing include data generalization, transformation, encryption, and hashing.

To consider PD as effectively pseudonymized, four cumulative criteria should be met (Figure 2):[12]

1. No individualization is possible, yet the individual can be singled out using additional information (ie, key to the code).
2. The key to the code must be kept confidentially by the data exporter (who might be a data controller or data processor) and typically at the investigational sites of a clinical trial.
3. Appropriate safeguards must be implemented to avoid data breaches and render control over PD to the exporter.
4. A thorough analysis must ensure that it is impossible to single out the individual even in case of cross-reference, considering the availability of such data.

Pseudonymized data are not directly identifiable data. Nonetheless, medical writers might have access to instantly recognizable PD when editing documentation for real-world evidence, clinical study reports, safety reports, and case reports. Therefore, it is essential that medical writers (freelancers or companies providing medical writing services) set up transparent pseudonymization methodology and adapt security measures to protect PD (Table 1). Importantly, pseudonymized data should not be considered anonymized data. The GDPR defines anonymous data as "information which does not relate to an identified or identifiable natural person or to PD rendered anonymous in such a manner that the data subject is not or no longer identifiable,"[1] and anonymized PD does not fall in the purview of the GDPR. The EU Data Protection Working Party, an independent European advisory body on data protection

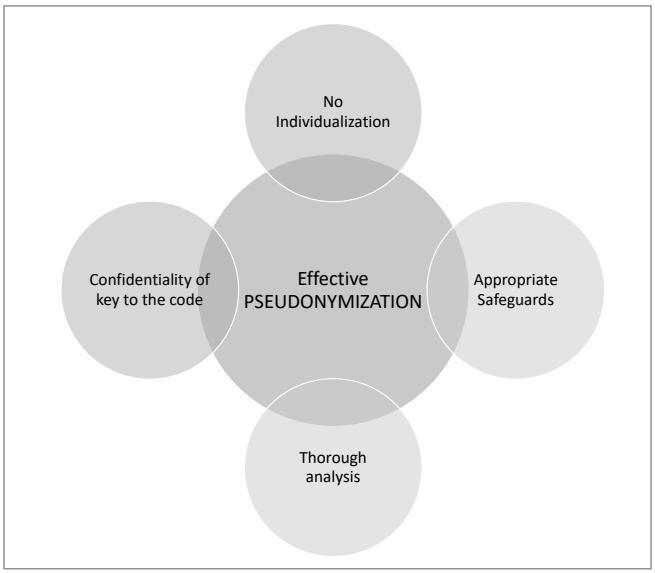

Figure 2. Four cumulative criteria to consider personal data effectively pseudonymized.

and privacy, analyzed several anonymization techniques and issued opinions regarding each method and the persistence of residual risk to identify the person.[12] In practice, it is impossible to achieve complete anonymization, and the success of reidentification in incomplete datasets is high.[13,14]

Security measures can be categorized into technical, organizational, and physical security measures, underpinned by strong contractual agreements (Table 1). Technical controls involve IT-related measures designed to protect data from unauthorized access, alteration, or destruction. Organizational controls include policies and procedures that govern how data are handled within an organization. Policies and procedures for data protection aim to manage:

- access to databases containing PD, that is, Electronic Case Report Forms (eCRFs), Electronic Data Capture (EDC), Trial Master File, safety data bases, as well as access to data during archival period;
- PD breaches, analysis of risks triggered by data breaches and evaluation of necessity whether the PD breach should be notified to Data Protection Authorities;
- data retention periods for different categories of PD based on the applicable regulatory requirements and the purposes of processing; the processes of data retrieval during storage and data deletion upon termination of the storage duration; and
- requests from data subjects.

The policies and procedures should be regularly reviewed and updated to reflect any changes in legal and regulatory requirements.

Physical controls refer to measures designed to safeguard the hardware and physical facilities in which data are stored. These controls protect critical components, such as servers, from physical threats and ensure the security of PD.

Contractual security is of utmost importance. Contractual frameworks serve as an instrument to demonstrate compliance with the GDPR by establishing clear responsibilities and expectations between parties involved in data processing (Figure 1). The DPA includes clauses on data

Table 1. Nonexhaustive Checklist of Organizational, IT, and Physical Security Measures to protect PD

Organizational Measures	Technical (IT) Measures	Physical Security Measures	DPAs
❑ Set up a data protection policy. ❑ Set up a data breach procedure describing step-by-step actions to contain the breach. ❑ Set up data retention, archival, and data removal or destruction procedures. ❑ Set up clear data management procedures that state how, to whom, by whom, and under what circumstances personal data can be accessed, erased, or sent back to the sponsor. ❑ Make personnel aware of the policies and procedures related to data protection. ❑ Regularly review and update data protection policies and procedures. ❑ Set up regular data protection trainings ❑ Raise privacy culture.	❑ Ensure control and restriction of access to the sources containing PD. ❑ Limit the number of users who may have access to PD. ❑ Limit time of access to PD. ❑ Use robust passwords to secure Internet connections. ❑ Install malicious software protection on workstations. ❑ Encrypt data and define ownership of the encryption keys. ❑ Define traceability methods to track the logs to the documents containing PD.	❑ Ensure the physical security of servers and platforms of data exchange. ❑ Ensure physical security of workstations. ❑ Set up procedures for managing paper format containing PD. ❑ Set up policies describing how to manage the physical maintenance of hardware. ❑ Set up procedures describing actions against the physical nonhuman source of risk (eg, earthquake zone).	❑ Use DPAs in contracts with controllers, processors, and freelancers who handle personal data. ❑ Clearly define responsibilities and liability of each party. ❑ Use adequate clauses to transfer data outside the EU to other countries.

DPA, data protection agreement; IT, information technology; PD, personal data.

protection obligations, breach notification procedures, and the implementation of security measures. Importantly, when PD are being transferred outside of the EU to countries that don't have an adequate level of data protection, contractual clauses ensuring appropriate data protection measures shall be used. For this matter, European Commission issued standard contractual clauses that can be used to legally frame data transfers to these countries.[11]

CONCLUSION

Medical writers, whether working for companies or as freelancers, often fall into the category of data processors under the GDPR. As such, their responsibility extends beyond creating accurate medical content—it includes protecting the PD of EU residents. The GDPR provides a broad description of security measures that controllers and processors must implement. Hence, companies can adapt those measures according to size, organization, budget, and type of processing activities. The main goal of the GDPR is to ensure that the risks of data breaches, which might have harmful consequences for individuals, are decreased and that individuals' rights to data protection are upheld. Medical writing plays an essential role in the disclosure of medical information and results of clinical studies, as well as having access to an individual's data, including sensitive and directly identifiable data. Therefore, it is essential that the medical writing community raises awareness about data protection among its members and beyond and does not underestimate the role of medical writers in safeguarding privacy.

Acknowledgments

The author thanks Cristina Draguta, Esq, and Andrea Karambelas, PhD, for proofreading.

Author declaration and disclosures: *The author is employee of MyData-TRUST, which provides services for compliance with data protection laws focusing on GDPR in the life sciences sector.*

Author contact: *revenco.tanya@gmail.com*

References

1. EU countries. European Union. Accessed on May 18, 2024. https://european-union.europa.eu/principles-countries-history/eu-countries_en
2. Types of legislation. European Union. Accessed on May 18, 2024. https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
3. Regulation – 2016/679. Updated April 27, 2016. Accessed on January 25, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
4. Reference methodology MR - 001: Health research requiring consent. National Commission for Information Technology and Civil Liberties (CNIL). Accessed January 25, 2024
5. *External Guidance on Implementing the European Medicines Agency Policy on Publishing Clinical Data for Medicinal Products for Human Use*. Version 1.4. European Medicines Agency, 2018. Accessed January 25, 2024. https://www.ema.europa.eu/en/human-regulatory/marketing-authorisation/clinical-data-publication/support-industry/external-guidance-implementation-european-medicines-agency-policy-publication-clinical-data
6. The Case Reports (CARE) guidelines. CARE. Accessed January 25, 2024. https://www.care-statement.org
7. Roguljić M, Ščepanović R, Rees M. Writing case reports, consent for publication and General Data Protection Regulation (GDPR). *Case Rep Womens Health*. 2020;27:e00204.
8. Regulation (EU) no 536/2014 of the European Parliament and of the Council of April 16, 2014, on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. EUR-Lex. Updated May 12, 2022. Accessed January 25, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02014R0536-20221205
9. Regulation (EC) no 1394/2007 of the European Parliament and of the Council of November 13, 2007, on advanced therapy medicinal products and amending Directive 2001/83/EC and Regulation (EC) No 726/2004. Updated July 26, 2019. Accessed January 25, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02007R1394-20190726
10. Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 on Medical Devices, Amending Directive 2001/83/EC, *Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and Repealing Council Directives 90/385/EEC and 93/42/EEC*. European Union, 2017. Accessed on January 25, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745
11. Standard contractual clauses (SCC). European Commission. Accessed on May 18, 2024: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en#eu-standard-contractual-clauses
12. *Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques*. European Union, 2014. Accessed January 25, 2024. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
13. Bentzen HB, Castro R, Fears R, Griffin G, Ter Meulen V, Ursin G. Remove obstacles to sharing health data with researchers outside the European Union. *Nat Med*. 2021;27(8):1329-1333.
14. Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. *Nat Commun*. 2019;10(1):3069.