Medical Communications and Writing for Patients

Editorial

Dear All,

This edition of *Medical Writing* offers a summary of a really excellent Meet and Share hosted by the Communicating with the Public Special Interest Group (CwP SIG). This Meet and Share explored the legalities around the EU General Data Protection Regulation (GDPR), EMA Policy 0070, and the newly emerging AI legislation, all of which were beautifully explained by Veronica K. Contreras, who is an expert in data protection, cybersecurity, and AI.

Together, GDPR, EMA Policy 0070, and the evolving AI legislation aim to advance scientific research, protect individuals' rights, and promote public health by fostering a well-informed and responsible approach to data management and technology use. Medical writers play a crucial role in ensuring compliance with these laws and regulations.

I'm incredibly grateful to Veronica for sharing her experience and knowledge so thoughtfully, and for answering all of our questions with such grace, patience, and humour! This is certainly a rapidly evolving field, and it takes a lot of time and effort to keep up.

I hope that you enjoy Veronica's article as much as I did, and in the meantime, stay safe and sane – enjoy the sunshine (if you have any!), and see you in the December issue!

Bestest, Lisa

SECTION EDITOR

Lisa Chamberlain James
lisa@trilogywriting.com

Communicating with the Public Special Interest Group Meet and Share: An overview of the EU General Data Protection Regulation, the EMA Policy 0070, and how they relate to AI

Veronica K. Contreras
Veronica K. Contreras, P.C.

doi: 10.56012/olsq3875

Correspondence to:
Veronica K. Contreras
veronica@vkc-pc.com

On December 3, 2024, Veronica K. Contreras, P.C., a firm that specialises in data protection, cybersecurity, and AI consulting services, had President and Founder Veronica Contreras give a presentation to EMWA.

The focus of this presentation was to provide an overview on the European Union (EU) General Data Protection Regulation 2016/679 (GDPR), the EMA Policy 0070, Artificial Intelligence (AI), and practical considerations on how best to apply the various laws and regulations in day-to-day business activities.

GDPR overview

The GDPR applies to entities in the EU, and those outside the EU, offering goods or services to individuals who reside in the EU or monitor individuals' behaviour within the EU. Under the GDPR, it is important to understand key concepts, and their applicability, for complying with the regulation. Key concepts not only include core definitions under the regulation, but also account for key principles, and other compliance requirements, that companies need to consider when conducting business in the EU and using individuals' personal data as part of companies' business activities and operations, inclusive of conducting, and supporting, clinical research. Key definitions include:

- **Processing**, i.e., includes various activities such as data handling, data collection, data storage, use, and destruction of personal data;
- **Personal data**, i.e., information relating to an identified or identifiable person, including pseudonymised data (coded information such as a patient ID number);
- **Sensitive personal data**, i.e., special categories of personal data, such as biometric characteristics, genetic data, religious beliefs, racial origin, medical health, political opinions, and data of minors under 16;
- **Data controller**, i.e., an entity that determines how personal data are processed;
- **Data processor**, i.e., an entity that processes personal data as instructed by a data controller; and
- **Subprocessor**, i.e., an authorised third-party to carry out processing activities on behalf a data processor's behalf.

Key principles under GDPR are designed to protect individuals' personal data and limit how such data may be processed by companies. These principles include:

- **Lawfulness, fairness, and transparency**, i.e., personal data must be processed fairly, in ways that individuals would reasonably expect and based on a lawful basis;
- **Purpose limitation**, i.e., personal data must only be collected for a specific purpose and only what is necessary for that purpose;

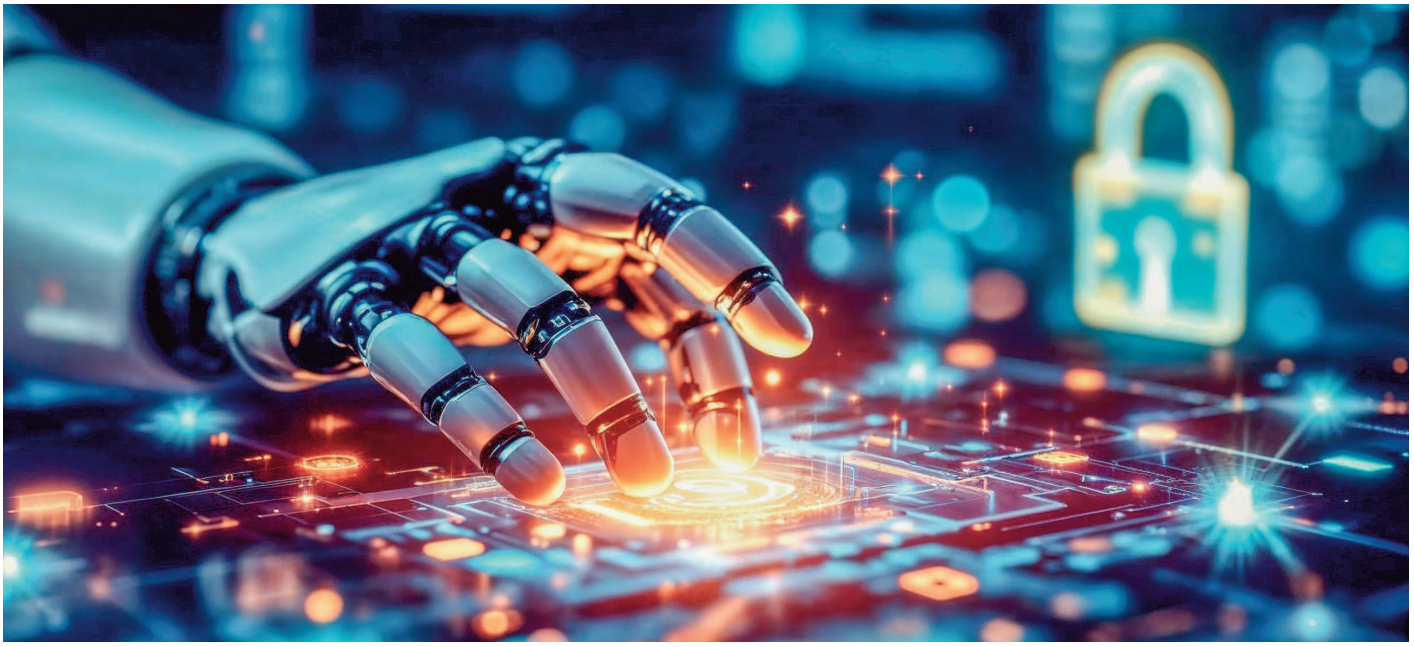

Photo: Freepik

- **Data minimisation**, i.e., ensuring that personal data collected are relevant, adequate, and limited to what is minimally necessary;
- **Accurate data**, i.e., personal data must be accurate, and necessary steps must be taken to update, rectify, or delete inaccurate data;
- **Data retention**, i.e., personal data must only be kept as long as necessary for the relevant processing activity; and
- **Data security**, i.e., implement appropriate security measures to protect personal data from unlawful or unauthorised processing, and from accidental loss, destruction, or damage.

The GDPR also incorporates requirements that any personal data processing must rely on a legal basis to allow for a processing activity to occur. These legal bases include:

- **Consent**, i.e., individuals must give clear and explicit consent to process their personal data for a specific purpose;
- **Contract**, i.e., processing is necessary for a contract with an individual or for human resource management activities;
- **Legal obligation**, i.e., processing is required to comply with legal or regulatory obligations;
- **Vital interest**, i.e., processing is necessary to protect an individual's life in emergencies;
- **Public interest**, i.e., processing is necessary for tasks in the public interest or official functions;
- **Legitimate interest**, i.e., processing is necessary for an entity's legitimate interests unless overridden by the need to protect personal data;
- **Archiving/scientific public interest**, i.e., processing supports archiving, scientific research, or statistical purposes;
- **Publicly available**, i.e., processing involves personal data intentionally made public by an individual; or
- **Permissible**, i.e., processing is otherwise allowed by applicable laws and regulations.

Some core compliance requirements under the GDPR afford individuals the ability to control how their data may be processed by companies and incorporates protective operational measures that need to be integrated into companies' operating practices. These core compliance requirements include:

- **Records of processing activities (ROPAs)**, i.e., data controllers and processors must maintain a ROPA log of all processing activities, document- ing contact details of the data protection officer, legal basis for the relevant processing activity, data categories, data recipients, international data transfers, data retention timelines, and data security controls;
- **Data processing agreements (DPAs)**, i.e., a DPA is required whenever a data controller uses a data processor, or a data processor uses a subprocessor, to process personal data. DPAs must include timing requirements for data breach reporting, data security controls, data transfer mechanisms, and indemnification and liability requirements;
- **International data transfer requirements**, i.e., personal data transfers to a third country must meet compliance requirements, including adequate data protection, data security controls, compliant data transfer mechanisms, and enforceable rights and legal remedies;
- **Individuals' rights**, i.e., the GDPR provides individuals with privacy rights, such as access to information, erasure, rectification, restriction of processing, data portability, objection to processing, and protection from automated decision-making and profiling; and
- **Data breach notification**, i.e., data controllers must notify relevant authorities and affected individuals within 72 hours of becoming aware of a data breach if it poses a high-risk to individuals.

EMA Policy 0070 was initially launched in 2015 to meet the growing demand for transparency in clinical data that forms the basis of regulatory decisions.

EMA Policy 0070 overview

The EMA Policy 0070 applies to pharmaceutical companies that have submitted clinical data as part of a marketing authorisation application or post-authorisation procedure for a human medicine in the EU. The policy enhances transparency and enables public access to clinical data, including clinical study reports (CSRs), clinical summaries, protocols, sample case report forms (CRFs), information on statistical methods used, and individual patient data (IPD).

Photo: Freepik

The EMA Policy 0070 was initially launched in 2015 to meet the growing demand for transparency in clinical data that forms the basis of regulatory decisions. This policy ensures that clinical data are published in an anonymised format to protect trial participants' identities and commercially confidential information.

The original policy had two phases: Phase 1 focused on CSRs, while Phase 2 was intended for IPD. The first publication was submitted in 2016. However, the policy was suspended in 2018 due to Brexit operational changes and revised in 2019 to cover both CSR and IPD. It resumed in 2020 with condensed reporting requirements for COVID-19 medicines. In 2023, the policy was relaunched, and as of September 2023, clinical data submitted for initial Marketing Authorisation Applications (MAAs) containing new substances with a Committee for Medicinal Products for Human Use (CHMP) opinion, were made public. Clinical data related to COVID-19, and other public health emergencies, continue to be made public. As of the policy relaunch in September 2023, the policy remains unchanged in content and has only undergone procedural changes. While step 2, of the policy relaunch, was originally anticipated in 2024, the EMA postponed next step requirements until 2025.

These policy background points highlight the evolution, and current status, of the policy, and emphasize its role in promoting transparency in clinical data. Some key requirements of this policy include:

- Submitting data in a format compatible with the EMA's publication system and within specified timeframes;
- All clinical data submitted for publication must be anonymised to protect patient privacy and commercially confidential information; and

Submission must comply with specific anonymisation guidance on how anonymisation should be carried out and the level of anonymisation required.

Key considerations to comply with the policy's anatomisation requirements and maintain patient privacy and confidentiality include:

- Understanding the process involved in transforming data into a form where individuals are no longer identifiable, and reverse engineering is impossible. If data are truly anonymised, they are no longer subject to data protection legislation requirements;
- Pseudonymisation reduces the linkability of a dataset with the original identity of an individual (e.g., patient ID). However, pseudonymisation alone does not result in an anonymous dataset, and data protection rules still apply. It is considered a best practice for enhancing security-related measures;
- Applicants/marketing authorisation holders are required to submit anonymous clinical reports. The EMA recommends a balanced approach to achieving adequate anonymisation, factoring in the risk of re-identification of a patient against the need to maintain data utility. For example, special consideration should be given to rare disease/small population studies by measuring the risk of re-identification and adapting anonymisation accordingly;

- Effective anonymisation considers three criteria:
  1. the possibility to single out an individual;
  2. the possibility to link records relating to an individual; and
  3. whether information can be inferred concerning an individual. If a planned report does not meet these criteria, an evaluation of associated re-identification risks must be performed; and
- Anonymisation techniques only extend to trial participants. Investigator, sponsor staff, and MAH applicant personal data should be redacted per EMA guidance.

AI legislation overview

AI legislation is on the rise, with new laws being passed to define legal requirements for AI use. These laws aim to protect individuals from fraud, theft, discrimination, bias, disinformation, and unintended consequences of AI use. Examples include the EU AI Act, and within the United States (U.S.), there are states, such as Colorado and California, that have passed their own AI legislation, which places significant obligations on developers, and providers, of high-risk AI systems (e.g., systems that make or significantly influence "consequential" decisions within the healthcare industry), including compliance with safety, transparency, fairness, algorithmic dis-

crimination prevention, and human intervention and accountability standards

AI system developers, and providers, must ensure robust evaluations are completed which address not only AI legislation requirements, but also consider data protection and information security requirements. These assessments should include, among other things, information about:

- An AI system that it will not affect individuals' safety and are thoroughly tested to ensure they are effective and not harmful to individual users;
- Algorithms used in AI systems will not discriminate against any individuals (e.g., gender, race);
- Any AI system use must be transparent, with clear documentation that includes descriptions of a system's features, general AI use, responsible parties, and explanations about AI outcomes;
- AI use should provide individuals the opportunity to opt-out from an AI system use in favour of a human alternative, where appropriate and applicable;
- What data will be used to train an AI model, inclusive of any personal data or other proprietary information;
- Cybersecurity measures enabled within an AI system; and
- Adherence to copyright laws.

Practical considerations

The aforementioned laws and regulations highlight the importance of transparency in clinical research and the interconnectedness of various laws in promoting public health, which is why it's important to understand how all these laws must be considered, and applied (where relevant), as part of any company's standard operational practices within the scientific and clinical research community.

For example, given that most clinical trials rely on patient consent for an individual to participate in a clinical study, GDPR requirements must be considered as part of the patient consent process. Under GDPR, consent often provides the legal basis which allows collection of a patient's personal data, inclusive of any medical records that would be needed as part of the applicable clinical study. Complying with good clinical practices and adhering to GDPR becomes a balancing act to lawfully process personal data, comply with data minimisation requirements, and avoid secondary use. A patient consent form, among other things, needs to include what data will be collected, why it will be collected, and how it will be collected. The challenge lies in ensuring that only the minimum data necessary are collected to meet the needs of a study and publishing goals, as outlined within the relevant consent form. GDPR limits how clinical data may be repurposed, or analysed, for future use, i.e., secondary use. Any future processing data uses that were not outlined in the relevant consent form will be prohibited unless patients are reconsented or the data are anonymised.

For any medical writers, or other stakeholders in the scientific community that share their research publicly, consideration should be given to what protections are in place to protect those individuals' intellectual property.

The EMA Policy 0070 complements GDPR by requiring all clinical reports to remove patient identifiers, thus anonymising all patient information and eliminating the ability to retrace an individual's identity. The process of anonymisation removes GDPR requirements because fully anonymised data are no longer considered personal data. This allows companies to not only comply with requirements under the EMA Policy 0070 (anonymisation requirements) but also leverage data for other use cases, such as data aggregation activities, without having to potentially re-consent patients to use their data**.** This is why compliance with the EMA Policy 0070 is valuable, advantageous, and promotes transparency and other benefits to advance public health.

While AI has been used to support scientific research for several years and more companies are integrating this technology into other aspects of clinical research to expedite and improve efficiencies when conducting clinical studies and publishing research for public use, it is important to understand how this technology may leverage a person's intellectual property to train an AI system. The basis of creating, or developing, an AI system requires certain information to train an AI model. Developers sometimes will look to public sources, such as clinicaltrials.org, or PubMed publications, to train their AI models. For any medical writers, or other stakeholders in the scientific community that share their research publicly, consideration should be given to what protections are in place to protect those individuals' intellectual property. Some considerations include:

1. whether research should be made commercially available beyond the EMA Policy 0070 requirements;
2. what protections a company like PubMed offers to protect individuals' intellectual property;
3. whether the "fair use" principle under copyright law is allowable or avoidable;
4. what royalty arrangements are available if an author's entire publication is used within an AI system;
5. require author acknowledgment labelling as part of an AI system; and
6. consider only sharing publication materials as part of an online subscription arrangement.

Conclusion

In the EU, GDPR sets the foundation for data privacy by defining key principles, and legal bases, for processing personal data, while the EMA Policy 0070 enhances transparency in clinical research by requiring anonymisation of clinical data. AI legislation is evolving to address the challenges, and risks, associated with AI use, emphasising safety, effectiveness, transparency, and algorithmic discrimination protections. Together, these laws and regulations, aim to advance scientific research, protect individuals' rights, and promote public health by fostering a well-informed and responsible approach to data management and technology use. Understanding and applying these interconnected laws in day-to-day responsibilities is crucial for compliance and achieving the overall objective of advancing public awareness and scientific research.

Author information

Veronica, president and owner of Veronica K. Contreras, P.C. (VKC-PC), specialises in data protection, cybersecurity, and AI consulting services, with more than 15 years of experience. VKC-PC assists clients with developing and implementing global data protection, cybersecurity, and AI compliance programmes, including without limitation: compliance with GDPR, Health Insurance and Portability and Accountability Act (HIPPA), California Consumer Privacy Act (CCPA), the Network and Information Security Directive (NIS2), and the EU AI Act.