WHO Guidelines on AI in Health : Impacts on privacy and regulatory considerations

Charlotte Beck, le 12 juin 2024

The WHO released various guidelines and recommendations regarding the use of artificial intelligence for health. Among the covered topics, data protection is regularly addressed. These aspects will be developed in this contribution.

Regulatory considerations on artificial intelligence for health

Ethics and governance of artificial intelligence for health : Guidance on large multi-modal models

Benefits and risks of using artificial intelligence for pharmaceutical development and delivery

The integration of artificial intelligence (AI) into healthcare offers great potential for advancing medical research, improving patient outcomes, and optimizing healthcare delivery. However, this integration also presents significant ethical, legal, and privacy challenges. The World Health Organization (WHO) has recently issued three guiding documents addressing the challenges of AI use for health. This contribution seeks to provide an overview of these guidelines, focusing on aspects of data protection and privacy in general.

Regulatory Considerations on AI for Health

The WHO's 2023 document "Regulatory Considerations on AI for Health" highlights critical aspects of privacy and data protection in the regulatory landscape. Due to the vast amounts of data involved in the development and use of this technology, anonymization techniques are often less effective, and the multiplication of processing activities increases security risks. This is particularly true regarding genetic data. The current regulatory environment is diverse, with international, national, and regional laws overlapping, and specialized regulations providing specific requirements, such as the GDPR, which introduces further challenges related to consent and transborder data exchanges.

The main aspect developed in this guidance regarding privacy and data protection pertains to the necessity to document and be transparent. Institutions can strive to establish trust, by providing detailed documentation of their data protection practices. These policies should

also clearly outline the types of data collected, the roles of involved parties (data controllers or data processors), the applicable legal bases, and the collection methods. Additionally, in order to demonstrate the compliance of an activity, and where the processing relies on such legal basis, a description of the consent collection method may be described.

The disclosure of these policies allows for regulators to determine a "standard of practice" by the companies making them available, upon which compliance can be examined. Companies must disclose significant uses of personal information for algorithmic decisions, detailing data types, sources, and the technical and organisational measures implemented to mitigate risks.

Still in the topic of documentation and transparency, the principle of data accuracy is put forward. Aimed at developers of AI, the necessity to ensure "quality continuum", a concept that is reflected in Art. 5 GDPR (with the principles of "accuracy" and "accountability"), but also in the field of Quality Control, such as the ICH E6 (R2) Guidelines for Good Clinical Practice (see Section "5.5 Trial Management, Data Handling, and Record Keeping"). The idea is to ensure the accuracy of the information throughout its lifecycle. Applied to AI, this means that privacy needs to be taken into account from the design to the deployment of AI.

Apart from the performance of privacy impact assessments, required by Art. 35 GDPR and recommended by the NIST privacy framework, documentation is a central method to ensure transparency, where developers should take a central role. Similarly, the creation of audit trails and annotating AI models allows to describe the decision-making process, and contributes to the "explainability" of the outputs of a model, further enhancing its transparency.

Ethics and Governance of AI for Health

The WHO's 2024 document "Ethics and Governance of AI for Health : Guidance on Large Multi-Modal Models" outlines ethical principles to guide AI use in healthcare. These principles include protecting autonomy, promoting human well-being and safety, ensuring transparency and explainability, fostering responsibility and accountability, ensuring inclusiveness and equity, and promoting responsive and sustainable AI. This guidance emphasizes that privacy must be prioritized throughout the lifecycle of large multi-modal models (LMMs), from development to deployment, through the provision phase.

The main privacy risks in patient-centred applications include the potential for sensitive information to be shared, difficulties in erasing data, and the risk of third-party disclosures. Overdependence on LMMs can undermine trust in healthcare systems due to privacy and confidentiality concerns. Compliance with data protection laws and human rights obligations

is therefore essential, as LMMs often use personal data without proper consent. Additionally, the fulfillment of access, rectification, erasure requests may not be possible, removing the possibility for individuals to have control over their information.

To mitigate these risks, ensuring high-quality, diversified data while avoiding data colonialism – collecting data from low- and middle-income countries – is essential. Other recommended measures involve the inclusion of patient representatives in AI development, allowing human oversight and the ability to address privacy concerns effectively.

Regarding measures which can be taken by governments, the guidance mentions : the implementation of target product profiles ; the design of standards and requirements ; the development of pre-certification programs ; the performance of audits ; the consideration of environmental impacts ; the requirement of notifications of machine-generated content to manage AI systems effectively.

Benefits and Risks of Using AI for Pharmaceutical Development and Delivery

The WHO's 2024 document on "Benefits and Risks of Using AI for Pharmaceutical Development and Delivery" underscores the importance of privacy in data collection and usage, as well as informed consent. AI in this context involves sourcing data from existing datasets, but also from other new sources, such as "hospital systems, including cellular data and genetic information, and from social media".

The need for large amounts of data leads to several risks, including discrimination, manipulation, and exploitation based on health status. Additionally, sharing health data can undermine an individual's dignity, autonomy, and safety.

Another privacy risk in the use of AI in clinical trials is the necessity to collaborate with specialized third parties. This sub-contracting of activities requires the setting up of a contractual framework, requiring said sub-contractor to comply with certain standards applicable to pharmaceutical companies, which may be outside of their usual sector of activity. This could lead to concerns about the proper compliance with health-care standards of the third parties involved.

The source of the risks for individuals often come during data transfer, where cyber-theft, accidental disclosure, government exploitation, discriminatory health insurance terms, and exploitative marketing practices pose significant threats.

In clinical trials, the WHO emphasizes the necessity for obtaining informed consent, especially when AI analyses medical records or public data, such as data collected from social media. The involvement of technology companies in drug development raises significant concerns about their data-sharing practices and privacy protections. As mentioned above, these companies often operate in a less regulated environment compared to the biomedical domain, thus necessitating stricter rules to ensure ethical use of data.

Conclusion

With the slow developments in the regulation of AI, these guidance documents provide a basis for companies and institutions to start building their compliance programs. The importance of certain principles, such as transparency and accuracy, the necessity of informed consent and identification of risks for individuals, as well as the need for caution in the collaboration with big tech companies are clearly outlined.

Although the medical and research fields are probably the sectors which can earn the most out of leveraging AI, they are also the most vulnerable to impact individuals' rights to privacy. Some of the above-mentioned practices are already provided for in laws currently in force, such as the GDPR, and provide certain protections and remedies. For the others, efforts from both legislators and practitioners will be needed to make them effective.

Proposition de citation : Charlotte Beck, WHO Guidelines on AI in Health : Impacts on privacy and regulatory considerations, 12 juin 2024 *in* www.swissprivacy.law/305