Ethics of AI in global health research

Cape Town, 29&30 November 2022

Global Forum on Bioethics in Research

Governance paper
Regulation of health data for AI in Uganda

Harriet Nankya, Makerere University, Uganda

Context: Assessing Uganda's regulation of health data in reference to the World Health Organization's recommendations for health data protection in the development and application of AI.

Commentary

Artificial Intelligence (AI) holds great promise to improve health. It can enable more accurate diagnosis and treatment of diseases, support pandemic preparedness and response, inform the decisions of health policy-makers or allocate resources within health systems[1]. However, to fully reap the benefits of AI, ethical challenges to its development and application must be addressed. Important issues to consider arise in the informed consent to use data, data safety and transparency, algorithmic fairness and biases, and data privacy[2]. This calls for the need to prioritize the ethical principles and human rights obligations by those who fund, design, regulate or use AI technologies for health, to avoid potential serious negative consequences.

The World Health Organization (WHO) in 2021 issued a report after analysing many opportunities and challenges of AI, and recommended policies, principles and practices for ethical use of AI for health and means to avoid its misuse to undermine human rights and legal obligations[1]. WHO hoped that these principles would be used as a basis for governments, technology developers, companies, civil society and inter-governmental organizations to adopt ethical approaches to appropriate use of AI for health. One of the key principles endorsed was protecting human autonomy; this principle requires, among other things, the protection of privacy and confidentiality of data and obtaining valid informed consent through appropriate legal frameworks for data protection.

This WHO endorsement points to the fact that the development of a successful AI system for health relies on high-quality data but systems can suffer with uneven management of such sensitive health data[3]. This presents several risks, for example, one's personal data may end up in the wrong hands or be used contrary to the owner's wish. Therefore, there is a need for data privacy and security in the research and implementation of AI-based health technologies, for compliance purposes and to build public trust in these solutions[4]. Currently in Uganda, just like in some other countries where technology advancement is still low, there are scant well-defined regulations in place to address the legal and ethical issues that may arise in the research and use of AI in health settings[2]. AI systems have been subject to sector-specific laws or subject-specific guidelines such as data-protection acts, cyber-security laws, anti-discrimination regulations. These measures have been applied on a haphazard and piecemeal basis creating large regulatory gaps and ethical implications of AI usage[3].

By basing on the WHO recommendations for health data protection in the development and application of AI, this paper describes how Uganda is positioned to comply with some of these recommendations on the regulation of health data for AI, as explained herein.

Recommendation 1*. Governments should have clear data protection laws and regulations for the use of health data and protecting individual rights, including the right to meaningful informed consent.*

Uganda passed the Data Protection and Privacy Act, 2019 ('the Act') in 2019 and the Data Protection and Privacy Regulations, 2021 ('the Regulations') in May 2021. The Act and Regulations are intended to support the protection of privacy and personal data through regulation of its collection, processing and storage. These privacy protections are already guaranteed to Ugandans under the Constitution and complement sectoral laws for regulated activities. The Act also guarantees the protection of privacy in the digital world. This Act mirrors the UK Data Protection Act, 1998 which revolves around several principles concerning data protection and collection. The Act is also in line with a number of international conventions including; the Universal Declaration of Human Rights to which Uganda is a signatory, the African Union Convention on Cyber Security and Personal Data Protection and the GDPR. It is also in line with the European Union General Data Protection Regulation (GDPR).

It is, therefore, very important for companies and other persons using AI and big data systems to abide by the strict requirements of the Act before collecting or processing personal data. This Act, manifests as a comprehensive law in regards to the AI technological advancements that could affect the right to privacy.

Recommendation 2. *Governments should establish independent data protection authorities with adequate power and resources to monitor and enforce the rules and regulations in data protection laws.*

Uganda has the Personal Data Protection Office (the Office) which is the national independent data protection authority. It is established as an independent office under the National Information Technology Authority, Uganda (NITA-U) responsible for overseeing the implementation of and enforcement of the Data Protection and Privacy Act No. 9 of 2019.

Section 3 of the Regulation stipulates that the Office, in the performance of its functions, is independent and not subject to the direction or control of any person or authority. Section 3(3)b of the Regulations points out that the affairs of the National Information Technology Authority, Uganda are managed separately from the affairs of the Office.

Section 5 of the Regulation stipulates the power of the office in carrying out the functions specified under the Act; In Section 5(a), the Office may establish a mechanism for collaboration and promotion of partnerships between various categories of players in the data protection and privacy aspects; and section 5(b) the Office will charge fees for services provided by the Office. In enforcing the regulations of the Act, Section 6 of the regulations stipulates that the Office shall cooperate with other government authorities like ministries, departments and agencies. The Office would, therefore, cooperate with agencies like; the Uganda National Council for Science and Technology (UNCST). UNCST is a government of Uganda Agency, established under the Ministry of Finance Planning and Economic Development to coordinate the formulation of national policy on all fields of science and technology, and for assisting in the promotion and development of indigenous science and technology[5]. UNCST works in collaboration with Uganda National Health Research Organization (UNHRO) for health research. With that stance, health research guided by UNCST and UNHRO is under the oversight of the Office.

In June 2022, The Office and the United Nations Capital Development Fund (UNCDF), launched a data protection and privacy portal that would ease reporting, processing, and resolving of data protection and privacy complaints and breaches[6]. The portal includes SMS/USSD functionality to enable universal access and usage by most citizens. UNCDF’s support to the Office to develop the data protection portal is part of its ‘Leaving No One Behind in the Digital Era Strategy’. The portal strategy, therefore, aims to empower millions to use digital services that will leverage innovation and technology to improve their wellbeing, while contributing to the Sustainable Development Goals.

The advent of AI and big data is set to raise a number of human rights issues. For example, the requirement for large volumes of data is likely to see the right to privacy of data being forsaken since the personal data of individuals is being shared and/or processed without their knowledge or consent. To counter this, NITA-U will have to step up its regulatory function to protect the integrity of personal data.

***Recommendation 3**. Governments should require entities that seek to use health data to be transparent about the scope of the intended use of the data.*

Section 12 of the Act states that; A person who collects personal data shall collect the data for a lawful purpose that is specific, explicitly defined, and is related to the functions or activity of the data collector, or data controller. Section 17 guides more on further processing of the data. It allows further processing of data but this should be specific to the purpose for which the data was collected (section 17 (1)). Section 17 (2) stipulates what should be put into account when further processing the data including; the relationship between the purpose of the intended further processing and the purpose for which the data was collected; the nature of the data concerned; the manner in which the data has been collected; the consequences that the further processing is likely to have for the data subject; and the contractual rights and obligations between the data subject and the person who processes the data (section 17 (3)(c)). Further processing of data is allowed for forensic purposes including national security, law enforcement etc. Further processing of data is also allowed for historical, statistical or research purposes (section 17 (3)(e)). Section 19 stipulated that for processing personal data outside Uganda**,** the data processor or data controller shall ensure that; (a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by the Act; or (b) the data subject has consented.

***Recommendation 4.** Mechanisms for community oversight of data should be supported. These include data collectives and the establishment of data sovereignty by indigenous communities and other marginalized groups.*

The Act doesn't stipulate community oversight of data. However, Section 9 highlights prohibitions on the collection and processing of special personal data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status, or medical records of an individual.

***Recommendation 5.** Data hubs should meet the highest standards of informed consent if their data might be used by the private or public sector, should be transparent in their agreements with companies, and should ensure that the outcomes of data collaboration provide the widest possible public benefit*

Neither the Act nor the Regulation stipulates data handling by the data hubs. However, Section 34 (1) of the Regulation stipulates that a data collector, data processor, or data controller who collects or processes personal data without the prior consent of the data subject in contravention of section 7(1) of the Act, commits an offense and is liable, on conviction to a fine not exceeding three currency points for each day that the contravention continues or to imprisonment not exceeding six months or both. Section 34 (2): Where the offense in sub-regulation (1) is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorizes the collecting or processing of personal data in contravention of section 7(1) of the Act, commits an offense and is liable, on conviction; to a fine specified in sub-regulation (1).

***Recommendation 6.** Governments should enact laws and policies that require government agencies and companies to conduct impact assessments of AI technologies, which should address ethics, human rights, safety and data protection, throughout the life-cycle of an AI system.*

In line with data protection impact assessment, Section 12 of the Regulation stipulates that;

- Subsection (1): Where the collection or processing of personal data poses a high risk to the rights and freedoms of natural persons, the data collector, data processor or data controller shall, prior to the collection or processing, carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data.

- Subsection (2): Every data protection impact assessment shall include (a) a systematic description of the envisaged processing and the purposes of the processing; (b) an assessment of the risks to personal data and the measures to address the risks; and (c) any other matter the Office may require.
- Subsection (3): The Office shall establish and make public a list of the processing operations which are subject to the requirement for a data protection impact assessment under subregulation (1).

Recommendation 7. *Governments, research institutions and universities involved in the development of AI technologies should maintain an ownership interest in the outcomes so that the benefits are shared and are widely available and accessible, particularly to populations that contributed their data for AI development.*

The Regulation has no clause on ownership nor benefit sharing of the outcomes. However, Section 26 of the Act stipulates that;

- Subsection (1): A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing.
- Subsection (3): Subject to subsection (1) a data subject may enter into agreement with a data controller for purposes of using or processing his or her personal data for pecuniary benefits.

Recommendation 8. *Governments should consider adopting models of co-regulation with the private sector to understand an AI technology, without limiting independent regulatory oversight. Governments should also consider building their internal capacity to effectively regulate companies that deploy AI technologies and improve the transparency of a company's relevant operations.*

In regards to data protection even for AI technologies, Section 6 of the Regulation stipulates the power of the Office to cooperate with other authorities.

- Subsection (1): The Office shall cooperate with other government ministries, departments and agencies in the implementation of the Act and regulations.
- Subsection (2): For the purpose of subregulation (1), all ministries, departments and agencies of government shall accord to the Office such assistance as may be necessary to ensure proper discharge of the functions.

Conclusion and recommendation

Principally, the rules and principles of the Act and the Regulation apply both in the phase of AI research and development and with regard to its use for analysing and decision-making about individuals. They contain important rights for data subjects relating to any processing of their personal data as well as obligations of processors, which will shape the way AI will be developed and applied. However, because AI, in a manner analogous to Big Data, presents a challenge for the application of traditional data processing principles, there is need to necessitate the elaboration of new applicative solutions to safeguard informational privacy and other fundamental right.

References

1. Guidance W. Ethics and Governance of Artificial Intelligence for Health. World Health Organization. 2021.
2. Naik N, Hameed BZ, Shetty DK, Swain D, Shah M, Paul R, et al. Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility? Frontiers in Surgery. 2022;9.
3. Väänänen A, Haataja K, Vehviläinen-Julkunen K, Toivanen P. AI in healthcare: A narrative review. F1000Research. 2021;10(6):6.
4. Sallstrom L, Morris O, Mehta H. Artificial intelligence in Africa's healthcare: ethical considerations. ORF Issue Brief. 2019(312).
5. Uganda U. Uganda National Council for Science and Technology (UNCST) Act (CAP 209). Kampala: UPPC. 1990.
6. Poor UPaPFft. Uganda Launches Data Protection & Privacy Portal to Streamline Management of Personal Data 2022.

This paper was prepared for GFBR 2022. Further details on the meeting are available at www.gfbr.global.