Implementation Guide for using the Model Law on Health Data Governance to Strengthen National Frameworks

SECTION 13: EMERGING TECHNOLOGIES

This section of the model law addresses the integration and regulation of emerging technologies in healthcare, focusing on safeguarding the rights of individuals and communities whose health data is collected, processed, or used by such technologies. As healthcare increasingly relies on advanced technologies such as artificial intelligence, machine learning, and big data analytics, it is imperative to ensure that these technologies are deployed in a manner that respects privacy, promotes equity, mitigates bias, and maintains transparency.

The section emphasises the need for individuals and communities to be fully informed about how their health data will be used in emerging technologies, ensuring that they can provide informed consent. Additionally, it sets out requirements for transparency and bias mitigation in the development and application of these technologies. The role of the Regulator is also highlighted, focusing on enforcing compliance with these requirements and collaborating with industry stakeholders to develop guidelines and best practices for scaling technologies in a way that does not compromise security or ethical standards.

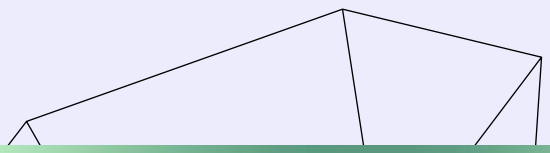
KEY DEFINITIONS

Emerging technologies is defined as novel and rapidly evolving tools, systems, and methodologies that harness computational advancements, data science or biomedical research to transform healthcare delivery, management, and decision-making. These technologies may include, but is not limited to, innovative computational models, artificial intelligence, machine learning, blockchain, and big data analytics.

RATIONALE

INFORMED CONSENT IN EMERGING TECHNOLOGIES

This provision ensures that individuals and communities are provided with clear, understandable information about the collection, processing, and use of their health data in emerging technologies. The requirement for informed consent aligns with the broader principle of autonomy and the right to control one's personal health data. In the context of emerging technologies, where the complexities of data processing can be difficult to understand, providing clear information is essential for enabling informed decision-making. This provision protects individuals and communities from potential misuse of their data and ensures that consent is genuinely informed.



TRANSPARENCY AND BIAS MITIGATION IN EMERGING TECHNOLOGIES

This clause mandates that all emerging technologies used in healthcare adhere to standards of transparency and undergo rigorous evaluation to identify and mitigate biases. Transparency involves making the underlying algorithms comprehensible to relevant stakeholders, while bias mitigation ensures that the technologies do not perpetuate or exacerbate healthcare disparities. Transparency is crucial for building trust in emerging technologies, particularly in healthcare, where decisions made by algorithms can have significant impacts on patient outcomes. By requiring that these technologies be understandable, and their limitations disclosed, the law ensures that stakeholders can make informed assessments of their use. Bias mitigation is equally important to prevent systemic inequalities from being embedded in technological solutions, thereby promoting equitable healthcare outcomes.

REGULATORY OVERSIGHT AND INDUSTRY COLLABORATION

This provision empowers the Regulator to enforce compliance with the transparency, bias mitigation, and informed consent requirements. It also mandates the Regulator to collaborate with industry stakeholders to develop guidelines and best practices for the responsible scaling of emerging technologies in healthcare. Regulatory oversight is essential for ensuring that emerging technologies are used responsibly and ethically. By authorising regular audits and assessments, the Regulator can monitor adherence to the law's standards and hold developers accountable. Collaboration with industry stakeholders is crucial for developing practical guidelines that balance innovation with the need for robust data security and ethical considerations.

OTHER OPTIONS OF FORMULATING THE SECTION

ENHANCED PUBLIC DISCLOSURE REQUIREMENTS

The section could include a requirement for public disclosure of the results of algorithm audits and bias mitigation efforts. This would enhance transparency and allow the public to hold technology developers accountable for their impact on healthcare.

INCENTIVES FOR ETHICAL INNOVATION

The law could provide incentives, such as grants or tax breaks, for companies that demonstrate a commitment to transparency, bias mitigation, and informed consent in their development of emerging technologies. This approach would encourage ethical innovation in the healthcare technology sector.

CREATION OF AN INDEPENDENT OVERSIGHT BODY

Instead of placing all oversight responsibilities on the Regulator, this section could establish an independent body dedicated to monitoring the use of emerging technologies in healthcare. This body could have a multidisciplinary team of experts to evaluate the ethical and technical aspects of these technologies.

NOTES ON INTERACTION WITH OTHER SECTIONS

HEALTH DATA COURT (SECTION 6)

Disputes related to the transparency, bias, or consent issues in emerging technologies may fall under the jurisdiction of the Health Data Court. The Court's role in adjudicating such matters ensures that the legal protections established by this section are effectively enforced.

INDIVIDUAL RIGHTS; PORTABILITY OF ELECTRONIC MEDICAL RECORDS (SECTION 7)

The informed consent requirements in this section align with the individual rights established in section 7, particularly the right to control personal health data. Both sections emphasise the importance of clear, understandable communication about how health data is used.

PROHIBITION ON RE-IDENTIFICATION (SECTION 8)

The transparency and bias mitigation requirements for emerging technologies are supported by the prohibition on re-identification in Section 8. Ensuring that health data cannot be re-identified without consent reinforces the ethical use of emerging technologies.

SUBSIDIARY LEGISLATION AND GUIDELINES (SECTION 17)

The development of guidelines and best practices for scaling emerging technologies will likely be detailed in subsidiary legislation. The adaptability of these guidelines to emerging needs and technologies will be crucial for the long-term effectiveness of this section.

DEVELOPING MECHANISMS AND GUIDELINES

REFERENCE DOCUMENTS

The Regulator should consult specific international standards and frameworks, such as:

- **OECD AI Principles:** These principles provide guidance on the responsible development and use of artificial intelligence, emphasising transparency, fairness, and accountability.
- **WHO Guidelines on Digital Health:** These guidelines offer a comprehensive framework for the integration of digital health technologies, with a focus on equity, ethics, and data protection.
- **ISO/IEC 27001 and ISO/IEC 27701:** These international standards provide guidelines for information security management and privacy information management, ensuring that emerging technologies are aligned with global best practices in data security.

STAKEHOLDER ENGAGEMENT

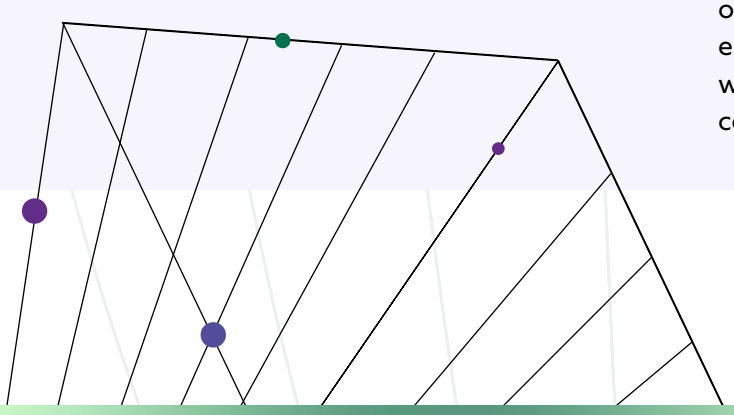
In developing these guidelines, it is essential to engage with a broad range of stakeholders, including technology developers, healthcare providers, patient advocacy groups, and data protection experts. Their input will help ensure that the guidelines are both practical and reflective of diverse perspectives.

CONTINUOUS MONITORING AND ADAPTABILITY

The guidelines should include mechanisms for continuous monitoring and regular updates to address new challenges and opportunities presented by technological advancements. This will ensure that the law remains relevant and effective in a rapidly evolving field.

FOCUS ON INTEROPERABILITY AND DATA SECURITY

The guidelines should emphasize the importance of interoperability and data security, ensuring that emerging technologies can integrate seamlessly with existing healthcare systems without compromising data protection principles.



INTERNATIONAL CONSIDERATIONS

The section's emphasis on safeguarding the rights of individuals and communities, particularly concerning the collection, processing, and use of health data, is directly dependent on existing international data protection frameworks. International organisations like the OECD and UNESCO have developed AI principles and guidelines that emphasise ethical AI use, fairness, accountability, and transparency. WHO also provides guidance on AI in healthcare. The UDHR and the ICCPR provide a foundation for protecting individual rights, including privacy, autonomy, and the right to informed consent. The section's alignment with these international human rights standards is crucial, as it ensures that the use of emerging technologies does not infringe on fundamental rights. The use of health data by emerging technologies often involves cross-border data flows, which are regulated by international trade agreements and treaties. For example, agreements such as the US-Mexico-Canada Agreement (USMCA) and the EU's data transfer agreements set out rules for the cross-border transfer of data, including health data. Ensuring compliance with these agreements is essential for maintaining lawful data flows and avoiding trade barriers. The European Commission's Ethics Guidelines for Trustworthy AI and similar frameworks from the IEEE or the World Economic Forum outline best practices for the ethical use of AI. International collaborations, such as those facilitated by the WHO, the International Medical Device Regulators Forum (IMDRF), or the Global Harmonisation Task Force (GHTF), aim to harmonise regulations across countries to ensure the safe and effective use of medical technologies. These efforts are crucial for developing coherent and globally recognised regulatory standards. In addition, international treaties such as the TRIPS Agreement could influence how intellectual property rights are managed in the context of emerging technologies. This includes the protection of algorithms, software, and databases that are integral to AI and machine learning in healthcare. Lastly, frameworks like the NIST Cybersecurity Framework (used internationally) and ISO/IEC 27001 standards provide guidelines for securing information systems. Adhering to these standards is critical for protecting health data from breaches and cyberattacks, particularly when technologies involve sensitive health information.

IMPLEMENTATION TIPS

This section is closely connected with any law regulating the implementation of Artificial Intelligence (AI) and care must be taken to integrate this section with the AI law. In addition human capacity to:

- Identify emerging technologies,
- Draft proposed regulations,
- Consult with industry stakeholders,
- Develop guidelines and best practices

must be developed. These functions would normally be embodied in public / private partnership where representatives of the healthcare industry, the state and relevant stake bodies meet on a regular basis to create and review regulations relating to emerging technologies.

This document was developed by Transform Health. This work was funded by the Patrick J. McGovern Foundation and Fondation Botnar.

Transform Health is a global coalition of organisations that work to harness the potential of digital technology and the use of data to achieve universal health coverage (UHC) by 2030. To learn more about Transform Health visit: www.transformhealthcoalition.org.

Transform Health