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

SECTION 8: PROHIBITION ON RE-IDENTIFICATION

This section establishes a critical safeguard in the governance of health data by prohibiting the re-identification of individuals from anonymised or pseudonymised health data. Anonymisation and pseudonymisation are key techniques used to protect individuals' privacy by removing or masking personally identifiable information from datasets. However, as data analytics and technology advance, the risk of re-identifying individuals from such datasets increases, potentially compromising privacy and leading to unintended consequences.

The prohibition on re-identification reflects a strong commitment to protecting the privacy and confidentiality of individuals whose health data is included in anonymised or pseudonymised datasets. By making it illegal to intentionally re-identify data, this section helps to maintain the integrity of privacy protections and fosters trust in the data governance framework. It ensures that health data can be used for research, public health, and other beneficial purposes without exposing individuals to the risk of being identified against their will.

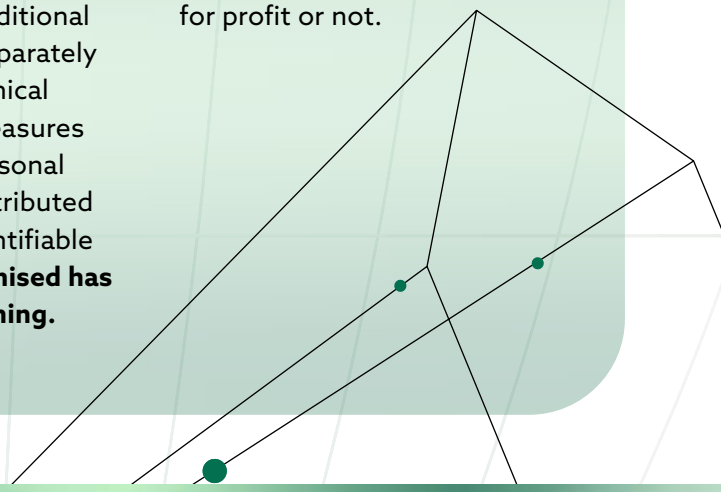
In line with a custodianship approach to data governance, this section places a legal and ethical duty on those who hold or process anonymised or pseudonymised health data to respect the privacy rights of individuals. It underscores the principle that health data, even when anonymised, should be handled with the utmost care and responsibility. By establishing clear prohibitions and accountability measures, this section aims to prevent the misuse of health data and protect the fundamental rights of individuals, reinforcing the ethical foundations of health data governance.

KEY DEFINITIONS

Anonymisation means the process of irreversibly transforming personal health data into a form in which the individual to whom the data relates cannot reasonably be identified, directly or indirectly, while still allowing the data to be used for legitimate purposes. **Anonymised** has a corresponding meaning.

Pseudonymisation means the processing of personal health data in such a manner that the personal health data can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal health data are not attributed to an identified or identifiable individual. **Pseudonymised has a corresponding meaning.**

Re-identification means the process by which information is attributed to anonymised or pseudonymised personal health data in order to identify the individual or community to whom the de-identifiedoperate for profit or not.



RATIONALE

PROHIBITION ON RE-IDENTIFICATION

The primary intent of this provision is to protect the privacy and confidentiality of individuals whose personal health data has been anonymised or pseudonymised. Personal health data is highly sensitive, and by placing a clear prohibition on re-identifying such data without permission, this section ensures that the model law goes beyond general data protection laws in safeguarding individual privacy. Anonymisation and pseudonymisation are key techniques for safeguarding personal data in research and healthcare. This prohibition is crucial for maintaining the integrity of these processes and ensuring that individuals' data remains protected, even when used for secondary purposes like research.

AUTHORIZATION OF ROBUSTNESS TESTING

This provision allows holders of proprietary rights in digital instances containing personal health data to authorize testing of anonymisation or pseudonymisation processes. This ensures that the techniques used are effective and can withstand attempts at re-identification. Robustness testing is essential for ensuring that anonymisation and pseudonymisation processes are secure. It allows data holders to identify and address vulnerabilities before they can be exploited, thereby reinforcing the protection of personal data.

REPORTING VULNERABILITIES

This clause obligates individuals or entities that discover vulnerabilities in anonymised or pseudonymised data to report them to the relevant parties, including the Regulator. This helps in the early identification and mitigation of risks associated with potential re-identification. Prompt reporting of vulnerabilities is critical for proactive risk management. It enables data holders and regulators to take timely actions to protect personal data, thereby minimizing the potential for harm.

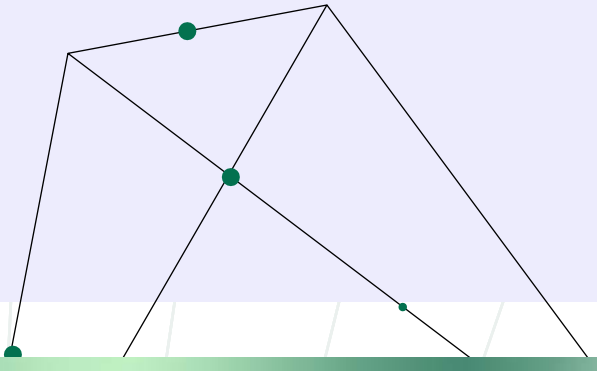
OBLIGATION TO ADDRESS RE-IDENTIFICATION RISKS

This provision requires holders of proprietary rights in digital instances containing personal health data to assess and address re-identification risks once they are informed of them. This ensures that data protection measures are continually strengthened in response to emerging threats. This ongoing obligation reinforces the dynamic nature of data protection, recognizing that security measures must evolve as new vulnerabilities are discovered and helps maintain the overall security of health data.

DISCRETIONARY LIFTING OF THE PROHIBITION BY THE HEALTH DATA COURT

This clause provides a mechanism for the Health Data Court to lift the prohibition on re-identification in specific cases, where justified, and under certain conditions. This ensures flexibility in the application of the law, allowing for exceptions in situations where re-identification may be necessary, such as for public health research or legal investigations. This flexibility is important for balancing privacy protection with the need for legitimate access to re-identified data in exceptional cases. It provides a legal pathway for controlled re-identification while safeguarding the interests of affected individuals.

Should the Health Data Court not be established, it is crucial that either existing courts or the Regulator be mandated to potentially lift the prohibition on re-identification under certain conditions, which can be specified. This ensures that there is always a legal mechanism in place to address exceptional cases where re-identification is necessary.



OTHER OPTIONS OF FORMULATING THE SECTION

MANDATED INDEPENDENT AUDITS

Instead of relying solely on the holder's authorization for robustness testing, the section could mandate periodic independent audits of anonymisation and pseudonymisation processes. This would ensure a higher level of scrutiny and reduce the risk of vulnerabilities being overlooked.

AUTOMATIC TRIGGER FOR RE-ASSESSMENT

The law could specify that any reported vulnerability automatically triggers a mandatory re-assessment of the anonymisation or pseudonymisation process, rather than leaving it to the discretion of the data holder. This would ensure a more consistent approach to addressing risks.

MANDATORY PENALTIES FOR NON-REPORTING

The section could explicitly include penalties for failing to report vulnerabilities within the specified timeframe. This would strengthen compliance and ensure that all parties take their reporting obligations seriously. The duty to report could also be inserted into section 14 (whistle-blowers).

MANDATED SELF-CERTIFICATION

The law could also provide that specific individuals must actively certify that reasonable tests have been conducted on the data to ensure it is anonymised and to provide the methodology used to arrive at the conclusion that the data is anonymised.

NOTES ON INTERACTION WITH OTHER SECTIONS

HEALTH DATA COURT (SECTION 6)

The role of the Health Data Court in potentially lifting the prohibition on re-identification ties this section directly to the Court's jurisdiction. The Court's ability to make exceptions ensures that the law can adapt to specific circumstances where re-identification may be warranted. If the Health Data Court is not established, this role should be assigned to existing courts or the Regulator.

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

The prohibition on re-identification supports the privacy rights established in Section 7 by preventing unauthorized identification of individuals in anonymised datasets, thereby reinforcing the confidentiality of their personal health data.

EMERGING TECHNOLOGIES (SECTION 13)

As new technologies are developed, they may present new methods for re-identification. This section must be adaptable to address these emerging threats, ensuring that protections remain robust against new forms of data analysis or manipulation.

OFFENCES AND PENALTIES (SECTION 15 AND 16)

Any breach of this section's provisions could be categorised under offenses related to unauthorised data use or gross failure to protect health data. The penalties section should reflect the seriousness of such breaches, providing for appropriate fines, sanctions, or other consequences.

INTERNATIONAL CONSIDERATIONS

The GDPR includes provisions that prohibit the re-identification of anonymised data, aligning with the principle that anonymised data should remain secure and that re-identification efforts should be illegal. The model law's prohibition on re-identification must be consistent with such international regulations to ensure compliance with global privacy standards. The IHR require member states to share health-related information during public health emergencies, but such data sharing must respect privacy and data protection principles. The prohibition on re-identification aligns with these international commitments to privacy protection in health data sharing. The OECD and WHO's guidelines on data sharing during pandemics guidelines encourage countries to implement robust data protection measures to facilitate cross-border data flows while safeguarding individual privacy. The prohibition on re-identification would need to comply with these guidelines, particularly when anonymised or pseudonymised health data is transferred across borders for research or public health purposes. Frameworks like the ISO/IEC 27001 for information security management systems and the NIST Cybersecurity Framework provide guidelines for protecting sensitive data, including ensuring that anonymised data cannot be re-identified. The section's prohibition on re-identification should align with these international standards to ensure that health data remains secure and protected from unauthorised re-identification attempts.

IMPORTANT CONSIDERATIONS

At a fundamental level, parties who have de-identified data need to be aware of the prohibition on reidentification and the data that may – when reidentified – be classified as "personal health data". This section will require a public enlightenment campaign to ensure data subjects are aware of this right and data controllers are aware of this duty.

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