AMA

AMA Position Statement

Data Governance and Patient Privacy in Healthcare

2022

This document outlines the AMA position on data governance and patient privacy. For the purpose of this Position Statement, data governance is defined as a documented set of processes, policies, standards and responsibilities that ensure the effective and efficient use of health data. Effective data governance frameworks guarantee the quality, security and privacy of the patient data that is collected, stored and shared.

1. Data Governance Overarching Principles

1.1. The AMA supports a connected healthcare system where data governance is patient centred and the use of data supports quality improvement.

1.2. The AMA believes that a connected, interoperable healthcare system must be based on principles of data safety, data quality, data privacy and data portability. A connected healthcare system that is based on equitable access to data is conducive to quality healthcare.

1.3. Effective data governance should ensure appropriate collection and use of data. Appropriate use of health data can enhance the provision of care for patients, improving health outcomes, increasing equitable and individualised care, while minimising duplication and gaps in care. This can improve productivity, efficiency and experience for health practitioners and provide evidence base for planning of care and services, both at the practice level and across the health system.

1.4. In the AMA view, there are three key aspects of effective data governance that must complement each other:

(a) Legal and regulatory framework,
(b) Technical data framework – data in a format that is appropriate, available at the right time, to the right person, with appropriate levels of data access control, and
(c) Ethical framework for data use.

1.5. Governance of digital health systems must enable safe and secure sharing of patient data across the healthcare settings while safeguarding patient privacy.

1.6. Indigenous data sovereignty principles must be obeyed when dealing with the health data of our indigenous population.[1]

1.7. Patients are the owners of their health data. Healthcare providers, private health insurance providers and clinical software developers/operators are the custodians of the patient data, not the data owners. As data custodians they must not be allowed to share or use these data outside the limits set by the national legislation. All reasonable efforts must be taken to guarantee the quality, security and privacy of the patient data.

1.8. With the rapid expansion of large international private technology companies into the healthcare space, the AMA calls for adequate regulation to ensure that patient privacy will be paramount, and that patient ownership of data is protected and enshrined in legislation.

1.9. The AMA calls for a broader national discussion around the privacy protections and ownership of data in the digital health systems, based on the General Data Protection Regulation (GDPR)

[1] https://aiatsis.gov.au/publication/116530

models of EU and UK, [2,3] with transparent limits on how, when, and by whom patient data can be accessed. In the interim, health data governance that is based on the Privacy Act and Australian Privacy Principles[4] should form the basis for any use of data contained in the digital health systems.

2. Data Governance Frameworks

2.1. Data governance frameworks applied by relevant entities in the healthcare space must demonstrate that patient data is handled in a transparent and accountable manner, with relevant privacy protections in place.

2.2. The AMA supports data governance frameworks that have clearly identified and stated data governance roles within relevant entities. Frameworks should define who can access data, the specific circumstances in which they can access the data, the purposes they can access and use data for, and how the data can be accessed.

2.3. Healthcare entities that collect and store patient data must ensure that there is a single source of truth – a single data repository, so that data is easy to find, access, use and share, within the relevant data safety and privacy principles.

2.4. Appropriate data governance should enable and ensure protection of the integrity of data, preventing unauthorised access to data, data loss, data modification or deletion.

2.5. Governance frameworks must ensure that all data use and requests for sharing of data must show demonstrable value in improving the healthcare system as a whole.

3. Ethical Use of Patient Data

3.1. The AMA supports ethical use of health data. The use of data must be for the public good and not present harm to individuals, the healthcare providers or the healthcare system, in line with the Quintuple Aims:

(a) Improved patient experience
(b) Better outcomes
(c) Lower costs
(d) Clinician wellbeing
(e) Health equity.[5]

3.2. Using patient health data in ways that result in increasing the profits of privately owned entities that are custodians of patient data, such as clinical software developers/operators and private health insurers, that is not in in line with the Quintuple Aims, will undermine consumer confidence in signing up to data sharing arrangements.

3.3. The AMA considers the use of patient health data to increase the profits of privately owned entities, that are custodians of patient data, unethical use of data and is strongly opposed to this.

3.4. The disclosure and linkage of health data must be limited to initiatives that exclusively aim to improve the health and health care of patients. Such initiatives would include health research, health policy analysis, health service program development and delivery, best practice health care, public health initiatives and the identification of unmet health service demand.

[2] https://gdpr.eu/what-is-gdpr/
[3] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
[4] https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference
[5] Itchhaporia D, et al. The Evolution of the Quintuple Aim. J Am Coll Cardiol. 2021 Nov, 78 (22) 2262–2264. https://doi.org/10.1016/j.jacc.2021.10.018

3.5. Only the data that are relevant for the above purposes should be shared and could include clinical diagnosis, types of services accessed, rates of service utilisation, risk factors, clinical indicators, current prescribed medications, vaccinations, allergies, and immunity status.

3.6. Medical practitioners must be informed and understand what health data they are the custodians of, be notified when it is extracted, who it is to be shared with, how it is to be utilised, and what accountability measures are in place in the event of breach of the terms of use. All of these components must be articulated in data sharing agreements.

3.7. Clinical software providers must not be allowed to impose conditions on doctors' access to patient data or impose shadow ownership of data by entering clauses in agreements with medical practices. Such behaviour is unethical and must be deemed illegal.

3.8. Patients and doctors that contribute the data must have confidence that their data is deidentified and not easily re-identifiable when it is shared for research or health system improvement purposes. Systems must ensure that the data on the doctors is not inadvertently released when performing big data research.

3.9. The AMA supports a form of ethics approval or compliance with national health research guidelines applying whenever health data are used without individuals' consent. Unless there is an enforceable requirement on data custodians to obtain ethics approval prior to the release of identified or identifiable health data under a data sharing agreement, these data should be exempt from data sharing.

3.10. The AMA does not support sharing health information (particularly MBS and PBS data) with private health funds outside the existing statutory schemes. Patients' medical information must be protected to maintain the clinical independence of their healthcare pathway.

3.11. Health data custodians should be subject to strong mechanisms to prevent security breach (e.g. data hacking) or misuse of patient data (e.g. threat to publish sensitive personal health information by hackers), or face legal penalties when/if breaches occur.

4. Data sharing patient consent

4.1. Patient consent for data sharing is a process by which the data owner and the data custodian agree to deidentified patient data secondary use and sharing for purposes other than the direct healthcare of the patient. This includes initiatives such as health research, health policy analysis, health service program development and delivery, best practice health care, public health initiatives and the identification of unmet health service demand.

4.2. Forms of consent activation must be agreed by the data owner and the data custodian. Ideally, this should be done using available technology platforms. Consent must not be activated unless verified by the data sender and the data receiver, to ensure that both parties have agreed terms of data sharing.

See also:

AMA Digital Health Vision Statement Preamble
AMA Position Statement on Health System Interoperability