Adoption of international privacy standards in New Zealand health information research

Vithya Yogarajan, Rajan Ragupathy

The use of patient health information in secondary research (henceforth referred as health information research) has many potential health and economic benefits for New Zealand, but patient privacy must be protected in the process. In this letter, we describe some exciting recent developments in data de-identification and international privacy law, and how these might impact health information research in New Zealand.

The way New Zealand district health boards (DHBs) handle, de-identify and release patient data for health information research has been described previously in this journal.[1] The DHBs self-report using various combinations of individual consent, ethics approval and data de-identification to meet New Zealand's legal and ethical requirements.[1] A model that strengthens New Zealand health information research by incorporating multiple safeguards has also been described.[2] However, as many health information research projects now cross jurisdictional boundaries, it is also worth considering overseas requirements when developing or reviewing New Zealand standards.

The European Union (EU) General Data Protection Regulation (GDPR)—which came into effect in May 2018—both poses challenges and creates opportunities for health information researchers across the world. The GDPR applies to EU residents and organisations located in EU member states but differs from the privacy laws of many other jurisdictions in that it also has 'extra-territorial' application. That is to say it covers the handling of EU residents' health information, even if those handling the information are not resident in the EU.[3–5]

Chapter 2 Article 9 of the GDPR includes health information among the 'special categories' of personal information, the processing of which is forbidden except under specific circumstances defined by law. New Zealand researchers wishing to collaborate with the world-class hospitals and academic institutions of the EU may therefore do well to consider GDPR from the outset.[3–5]

Certain key features of the GDPR should be kept in mind. The GDPR allows the reuse of health information for secondary research with the consent of the individual(s) concerned but stipulates that this requires 'affirmative consent'. (Simply failing to exercise an opt-out or ticking of a pre-filled box may not meet this requirement). However, the GDPR also allows 'broad consent' for particular areas of research and specifically permits the use of health data without consent for medical research that is 'in the public interest'.[3–5]

The GDPR also creates a higher barrier for data to be considered 'de-identified' (to the point that it is no longer considered personal health information) than New Zealand researchers may be used to. New Zealand's Health Information Privacy Code (HIPC) allows the use of health information for research without individual consent where the information is 'to be used in a form in which the individual concerned is not identified' (NB 'identified' as opposed to 'identifiable').[6]

What constitutes 'not identified' is not defined in the HIPC, but this could be considered equivalent to the relevant provisions in the US' HIPAA Privacy Rule.[6] The HIPPA Privacy Rule provides two standards by which health records could be de-identified to the point where they are no longer considered identifiable health information. The first is the 'expert determination' standard, where a suitably qualified expert examines the de-identified data and determines that the risk of re-identification of an individual is 'minimal'. The 'safe harbor' method is much more specific and lists 18 categories of identifiable information about the individual (as well as family and associates) that must be removed for a record to be considered de-identified.[7]

HIPAA's requirements have to date been considered the gold standard in developing automated de-identification systems.[8,9] Several systems have achieved the benchmark of 95% accuracy or higher overall across the 18 HIPAA 'safe harbor' categories in competitions, but it remains to be seen if commercial systems can replicate this this in real-world conditions . However, accuracy is lower for certain categories such as medical device identification numbers.[8] It has been shown that attackers can unmask considerable amounts of identifiable personal information if they gain access to even a small fragment of medical device data output.[10] Manual de-identification is an alternative but is impractical for large datasets due to the specialised training, time and personnel costs involved.[1]

The GDPR is arguably more stringent than HIPAA on the requirements for de-identification. It requires considering the possibility that a 'de-identified' record could be re-identified by other indirect means, such as cross-linking with other data sets, and considering technological developments that would increase the risk of re-identification. Under these standards, it is likely that datasets that have been de-identified to the standards of HIPAA's safe harbor provision—but have not had any additional safeguards such as aggregation or noise addition—would not meet GDPR standards.[11–12] It remains an open question whether a dataset could be de-identified to such an extent that re-identification is not possible while retaining full usability.[8]

While GDPR may pose challenges to New Zealand researchers seeking to work with EU data, it also creates opportunities by harmonising the data protection standards of EU member states.[3–5] As the GDPR de-identification requirements are arguably more stringent than those in HIPAA, datasets de-identified to EU standards would almost certainly meet US 'expert determination' and 'safe harbor' standards. Incorporating GDPR standards into New Zealand's own evolving health information standards (perhaps as an optional tier over and above those required by New Zealand law) may, therefore, make international collaborations more likely in future indeed.

Competing interests:

Nil.

Author information:

Vithya Yogarajan, Doctoral Assistant and PhD Student, Department of Computer Science, The University of Waikato, Hamilton, Waikato; Rajan Ragupathy, Clinical Trials and Research Pharmacist, Pharmacy Services, Waikato District Health Board, Hamilton, Waikato.

Corresponding author:

Mr Rajan Ragupathy, Pharmacy Services, Waikato District Health Board, Selwyn Street Entrance to Waikato Hospital, Selwyn Street, Hamilton.
rajan.ragupathy@waikatodhb.health.nz

URL:

http://www.nzma.org.nz/journal/read-the-journal/all-issues/2010-2019/2019/vol-132-no-1492-29-march-2019/7848

REFERENCES:

1. Yogarajan V, Mayo M, Pfahringer B. Privacy Protection for health information research in New Zealand district health boards. NZ Med J 2018 November 9; 131(1485):19–26.
2. Ragupathy R, Yogarajan V. Applying the Reason Model to enhance health record research in the age of ‘big data’. NZ Med J 2018 July 13; 131(1478):65–67.
3. Rumbold JM, Pierscionek B. The effect of the general data protection regulation on medical research. Journal of medical Internet research. 2017 Feb;19(2).
4. Chassang G. The impact of the EU general data protection regulation on scientific research. ecancermedicalscience. 2017;11.
5. International Association of Privacy Professionals. Territorial scope of the GDPR from a US perspective. [Online]. [Last accessed 31 Jan 2019]. Available from: http://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/
6. Office of the Privacy Commissioner. Comparison paper on health privacy laws. [Online]. [Last accessed 31 Jan 2019]. Available at: http://www.privacy.org.nz/news-and-publications/books-and-articles/comparison-paper-on-health-privacy-laws-2/
7. United States Department of Health and Human Services. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. [Online] [Last accessed 31 Jan 2019]. http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html
8. Yogarajan V, Pfahringer B, Mayo M. Automatic end-to-end de-identification: is high accuracy the only metric? [Online,archived paper] [Last accessed 31 Jan 2019]. Available at: http://arxiv.org/pdf/1901.10583.pdf
9. Yogarajan V, Mayo M, Pfahringer B. A survey of automatic de-identification of longitudinal clinical narratives. [Online, archived paper]. [Last accessed 31 Jan 2019]. Available at: http://arxiv.org/abs/1810.06765
10. Mayo M, Yogarajan V. A nearest neighbour-based analysis to identify patients based on continuous glucose monitor data. In Proceedings of the Asian Conference on Intelligent Information and Database Systems (ACIIDS 2019). Lecture Notes on Artificial Intellgence (LNAI), Springer, to appear.
11. Brasher E. Addressing the failure of annomyization: Guidance from the European Union’s General Data Protection Regulation. [Online]. [Last accessed 31 Jan 2019]. Available at: http://cblr.columbia.edu/addressing-the-failure-of-anonymization-guidance-from-the-european-unions-general-data-protection-regulation/
12. Polonetsky J, Tene O, Finch K. Shades of Gray: Seeing the Full Spectrum of Practical Data De-Intentification. Santa Clara L. Rev. 2016; 56:593.