Government response to the Privacy Act Review Report (https://consultations.ag.gov.au/integrity/privacy-act-review-report/)

Response 240164857

Back to Response listing (https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/published_select_respondent?show_all_questions=0&sort=submitted&order=ascending&_q__text=MTAA)

☐ Include unanswered questions

Questions about the submitter

Who are you making this submission for?

Please select one item

- ○ Myself
- ○ Another person
- ✔ Organisation (including Commonwealth, state, territory or local government agency)

What is your organisation?

Organisation

Medical Technology Association of Australia

What sector is your organisation a part of?

Please select one item

- ○ Private sector – small business
- ○ Private sector – medium to large business
- ✔ Representative body
- ○ Legal sector
- ○ Not-for-Profit sector
- ○ Government (including state and territory)
- ○ Academia

Personal information, de-identification and sensitive information

Should there be a criminal offence for re-identifying de-identified information? What exceptions should apply?

1.a)
There are concerns that a proposed criminal offence for reidentifying de-identified data would result in adverse impacts on how MedTech business currently conduct their operations. The proposed change would shift the balance, by removing the net benefits derived from re-identification in order to protect the individual's right to privacy. At the moment, re-identification of de-identified data enables MedTech companies to undertake activities that lead to improved delivery of healthcare and promotion of public health initiatives. Making reidentification a criminal offence would impede companies' abilities to undertake important activities that are in the public health interest and mean society could miss out the improvements in services and technologies. There should be exemptions in place if re-identification was to become a criminal offence. These would include where re-identification is required to fulfil legal and health obligations, a contractual obligation, or in cases where reidentification is inadvertent.

Should consent be required for the collection, use, disclosure and storage of other tracking data, such as health data, heart rate and sleeping schedule, in addition to precise geolocation tracking data?

1.b)
There should continue to be exemptions in place for MedTech companies in terms of collection, usage and storage of health information of health data, with the appropriate safeguards in place.
In addition, having broader exceptions to the consent requirement for industry led research would be beneficial in supporting more business activities that lead to better public health outcomes. However, there would need to be strong safeguards in place and would likely require a body that is familiar with managing healthcare data (such as the NHMRC) to develop a framework that could adopted by both government and industry to do activities in a way that complies with privacy requirements but does not require consent.

Small business exemption

If you are a small business operator, what support from government would be helpful for you to understand and comply with new privacy obligations?

Please select all that apply

- [x] Information sessions
- [x] Written guidance
- [x] Digital modules
- [x] Self-assessment tools
- [x] Financial rebates or tax concessions for obtaining independent privacy advice
- [ ] Other

Please expand on your response

2) Small business exemption
The current approach where a small business with an annual turnover of 3 million or less are exempt from the Act may not be appropriate going forward. In terms of upholding the rights of individuals, citizens expect have a high level of data protection regardless of the size of the company managing the data. This combined with the increase proliferation of new technologies and advanced sales and marketing tools leveraging personal information means an individual's privacy is at risk from multiple fronts.
Therefore, MTAA would encourage removal of the small business exemption on the condition that sufficient supports are provided to allow small companies to transition to comply with the Act . The largest barrier for small business and the increased regulatory and compliance costs and this is where the OAIC can best help support business undertaking this transitions. These supports, as outlined in the Privacy Act Review, 2022 which would include, as examples:
• Template privacy policies
• Tailored advice and targeted education by the OAIC
• Tax offsets commensurate to the cost of compliance

Employee records exemption

How should employers provide enhanced transparency to employees about the purposes for which their personal and sensitive information is collected, used and disclosed?

3a)
There is a sound basis in providing enhanced transparency to employees that does not require seeking consent each time employee data is processed. Enhanced transparency may be achieved in the following ways:
• During the interview process, as part of the employment contract including the privacy collection statement/ privacy policy document with the draft contract, and the during the onboarding process
• Setting out in the employment contract a comprehensive list of purposes for which employee

data will be collected, shared, transferred etc.
• Making an employee privacy policy accessible via an internal portal or internal guidelines/policy documents.
• Sending out company wide communication to update employees of ongoing initiatives/programs.
• Providing a neutral avenue for employees to communicate concerns/potential breaches of privacy through an Ethics helpline or portal (this could be organised by the OAIC)

If privacy protections for employees were introduced into workplace relations laws, what role should the privacy regulator have in relation to privacy complaints, enforcement of privacy obligations and development of privacy codes in the employment context?

3c)
The privacy regulator would be involved in investigative activity and in some instances the ability to make determinations while in other instances refer to the Fair Work Commission. Ideally this would require some harmonisation across the Fair Work Commission and OAIC.

Research

Should the scope of research permitted without consent be broadened? If so, what should the scope be?

6a/b
Rationale for broadening scope permitted without consent:
While an individual's right to privacy should be upheld at all times, this has to be balanced against important benefits that are in the public interest. Research is one of the areas in MedTech where a net health benefit is provided for society and requires a degree of flexibility in how personal information is obtained to achieve this.
The scope of research permitted without consent should be broadened and should be the same definition applied to government and industry (including MedTech) respectively, because of the important public health benefits it generates. Research not only helps in discovering novel technologies, which in turn improve society's overall health, it also helps with business improvement initiatives that also improve public health outcomes. For example, a business could find more efficient ways to deliver services leading to shorter wait times for health consumers to access products/ receive treatment. Similarly, a business might be able to enhance products' capabilities they are already providing through research they conduct, improving patient health outcomes.
AI's inclusion in the broader scope of research permitted without consent
Specifically, in MedTech, an important area of industry activity that should be included within the scope of research permitted without consent is use of artificial intelligence (AI) for two reasons. Firstly, AI helps in the development of smarter devices, highlighting AI's ability to enhance products/ improve services to deliver better patient outcomes. Secondly the use of AI, for this purpose, does not pose a fundamental risk to the privacy of the individual.
In terms of enhancing products/ services, managing diabetes provides a clear example of the benefits of applying AI. In this case, AI algorithms allow medical devices to go beyond simply tracking and reporting raw data, but to better guide and inform doctors and patients. A trained AI algorithm can identify among thousands of tissue-images the areas to focus on for possible malignancies. AI solutions, including subsets such as machine learning, can help diabetes patients in the following ways:
• better understand and predict their patterns and responses to nutrition and exercise,
• become more proficient with their insulin pump settings
• improve their "time in range" of appropriate blood glucose levels, a key indicator of effective diabetes management.

This provides greater freedom to patients, more peace of mind to parents and other care providers, and helps keep patients "in range", which is central to their health in both the long and short term.

In terms of the potential harms to privacy that could arise using AI to improve a MedTech product/ service experience, health data that is generated by AI is different. This is because health information using AI that is derived from a patient's personal information (e.g. internal body scans) is solely benefitting the AI by improving its technical capability to better treat the

patient – there are no other direct harms linked with generation of thins inferred health information to an individual.

Amending the secondary uses of health information

Currently, there are restrictions on the situations where health information can be disclosed for secondary purposes that are not explicitly stated at the time of data collection. This serves as a barrier for MedTech companies to leverage the data in other ways in the future that could help drive innovative activities that are critical to develop new products, techniques, or improve the quality of existing services. Furthermore, at the time of data collection, it may not be possible to anticipate all the potential uses of the data (including public health and pubic interest purposes).
Therefore, there should be a revision of the 'secondary use' definition involving removal of the requirement that there be a direct linkage to the purpose stated at collection. Instead, there should be a focus on allowing research to be conducted for emerging secondary outcomes post what was stated at collection that yield valuable health and educational outcomes.
For additional context, Australia can currently export research to other jurisdictions around the world where they are able to leverage the data in ways that are not allowed here locally (the use of data matching services and ability to retrospectively use data for other reasons). Already under the support for such initiatives and in countries such as Singapore and South Korea, there is a recognition that business improvement is a valid reason to process personal information. There is clearly an opportunity for Australia follow suit. However, there would need to be safeguards in place to ensure data from Australian MedTech research was used appropriately and an entity such as the NHMRC would be well suited to developing a framework that could apply both to government and industry.

Which entity is the most appropriate body to develop guidelines to facilitate research without consent?

6c)
The NHMRC would be well suited to developing a framework/ guidelines that could apply both to government and industry to facilitate research without consent.

Individual rights

What would the impact of the proposed individual rights be on individuals, businesses and government?

8a)
Right to erasure
An individual's right to erasure of their personal information involving MedTech would need to be thoroughly examined. There are many inadvertent outcomes that could occur if this right was enforced without understanding the contexts that this decision could be taking place in. For example, there might be certain medical technologies whose functionality depends on collecting and analysing personal information about the user. Similarly, there might be situations where is not feasible to erase data - this applies to Machine Learning in MedTech where the data is used to train a model. Once the model is trained a request of right to erasure is not possible because it is technically not feasible to expunge the learning from the model. Additionally, global Medical Device Regulatory authorities may have expectations that datasets used for training and development be kept for regulatory investigation purposes
Furthermore, certain studies carried out by MedTech companies (eg longitudinal studies) that require measuring particular health outcomes over many years/ decades could be disrupted by an erasure request, undermining the integrity of the research and its findings.
Another complication is how the right to erasure could be enforced if data has been shared across multiple stakeholders (common in the MedTech sector). There could be a situation where the primary user can enforce the request but how would this be actioned by third party that might be using only some of the personal information collected? Again, as highlighted earlier a clear understanding the controller and processor definitions would need to be provided.
Erasure requests may also impact the ability to provide patient care or meet contractual obligations with customers (an example of a current request: A company processes pacemaker transmission data in a system on behalf of the health care professional (HCP) and patient. The

main purpose is to transform the raw data into a report for the HCP on the function of the patient's heart. The company cannot – without significantly impacting that patients care – erase that patient from the system, or de-identify them, as the HCP will then not be able to receive the transmission data).
There are also challenges with maintaining documentation retention requirements if an erasure request is made. Significant quantities of personal information of a patient must be retained in order to provide appropriate, ongoing high-quality care to the person to whom the information relates and to document the care provided. Furthermore, the costs of implementation will be disproportionate to any privacy benefit to an individual. The existing de-identification regime is more appropriate for healthcare as to completely erase would also affect other legitimate purposes, research, quality improvement, trend reporting, assisting in Field Corrective Actions. The exceptions in 18.6 do not include those necessary for healthcare/reasonable expectation of safety etc

A direct right to action and Statutory Tort for serious invasion of privacy
There should not be a direct right to action or a Statutory Tort for Invasion of Privacy as it would divert resources operating in the health sector away from the health sector to managing potential claims under these proposals (vexatious claims will increase). These claims should be managed, or at least received and triaged in the first instance, by the OAIC. Litigation, by its adversarial nature and the Australian Courts large case load, is prohibitively high-cost, and has the potential to entrench parties' positions and lengthen dispute times.
This may result in potential inconsistency and uncertainty in the application of the Privacy Act, and risks class actions, which are an incomplete vehicle for issues where the "injury" is a subjective test of individual harm. If enacted, Individuals should have to seek leave to bring an action, which would be another way of limiting vexatious claims. There should also be a limitation period to provide for certainty.

Controllers and processors

If small business non-APP entities that process information on behalf of APP entities are brought into the scope of the Act for their handling of personal information on behalf of the APP entity controller, what support should be provided to small businesses to assist them to comply with the obligations on processors?

12) Controllers and processors
12a)
The main challenges for small businesses that would be brought into the Act processing information on behalf of an APP entity could be inability to appoint a full-time dedicated privacy officer or dedicated cybersecurity team.

Assistance could be provided in the form of providing a guide on developing a data management programme or providing some training materials on the same. In addition, a handbook on identifying common gaps in info-comm technology (ICT) systems so as to guard against common types of data breaches or providing a check list on the same.

Overseas data flows

Should the extraterritorial scope of the Act be amended to introduce an additional requirement to demonstrate an 'Australian link' that is focused on personal information being connected with Australia?

13a) Overseas Data Flows
The requirement to show an Australian link would be challenging where the requirement involves providing an exact location. The need for granularity when disclosing what types of information are going overseas in combination with the volumes of information involved would put a severe strain on resourcing for companies of all sizes.

Notifiable Data Breaches

How can reporting processes for Notifiable Data Breaches be streamlined for APP entities with multiple reporting obligations?

14a)
One possible way to streamline is to create an online portal with some unique identifier where organisations can upload reports when there is a Notifiable Data Breach

Should APP entities be required to take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a Notifiable Data Breach? If so, what factors should be taken into account when determining reasonable steps?

14b)
Yes, reasonable steps need to be taken, and could involve developing a Data Breach response plan and an Assessment Team that can help assess what is "reasonable". This because reasonable can mean different things in different circumstances (eg in a remote vs urban area). So notifying an individual via email in a remote setting might not be appropriate if there poor internet connectivity as an example.
Aim to contain the breach as quickly as possible and take immediate steps to limit any further access to or disclosure of personal data.
Record the data breach and organisation response in an incident report – it might help if this was done in a standardised way the capture key bits of information:
- Number of individuals affected
- Types of personal data disclosed
- Systems/ services affected
- If help is required to contain the breach

Attachments

Privacy Act Review - Medical Technology Association of Australia - Government response submission.pdf (https://consultations.ag.gov.au/integrity/privacy-act-review-report/consultation/download_public_attachment?sqId=pasted-question-1676440442.95-78210-1676440443.24-67813&uuId=240164857)