Private Healthcare Australia
Better Cover. Better Access. Better Care.

Privacy Act review

March 2023

Contact:

Ben Harris – Director Policy and Research
0418 110 863
ben.harris@pha.org.au

About Private Healthcare Australia

Private Healthcare Australia (PHA) is the Australian private health insurance industry's peak representative body. We have 24 registered health funds throughout Australia as members and collectively represent 98% of people covered by private health insurance. PHA member funds provide healthcare benefits for over 14 million Australians.

Introduction

Health funds are committed to protecting the personal information of their members in a manner that is appropriate in the digital age.

Health funds in Australia and globally are changing from being pure payors of claims to broadly supporting customers' health through wellbeing and prevention programs, advice, navigation, healthcare and rehabilitation delivery. This change is necessary as populations are ageing and people have more long-term conditions that need management. Funds are keen to promote better health and wellbeing which is essential to improve health of Australians, and consistent with the direction of healthcare around the world.

Customers expect their health fund to play a greater role in supporting their health. For example, if a fund can detect that a patient is potentially at high risk of a heart attack, a member would expect the fund to advise them and help them avoid this event. Therefore, it is important to ensure that privacy law does not inadvertently preclude the use of health data to deliver on consumers' expectations.

Funds use data (including members' personal information) for a broad range of permitted secondary purposes that provide benefits to their members, including:

- audits
- health prevention programs and advice
- research
- delivering health services
- automated decision processes, and
- analytics and efficiencies.

Each of these uses provide public benefit, including lowering the cost of private health insurance for fund members.

The proposed changes and associated guidance should not impede health funds from continuing to use members' personal information for these purposes in the future, so that they can continue to undertake their 'business as usual' activities and provide a broad range of health benefits, products and services to their members and to the wider community.

Funds want to use members' personal information for these purposes in the future, so that they can continue to undertake their business as usual activities and provide value to their members and to the community. Funds are also concerned about ensuring that the proposals consider the commercial implications for APP entities, potential population and individual health impacts, as well as the benefits to individuals.

Health funds already manage many overlapping legislative and regulatory regimes with effects on privacy. As funds are national organisations, there are up to nine Parliaments providing regulatory guidance, along with independent and semi-independent regulators such as the Australian Prudential Regulatory Authority (APRA), the Australian Competition and Consumer Commission (ACCC), the Private Health Insurance Ombudsman, the Australian Health Practitioner Regulatory Authority (AHPRA), the Australian Council for Health Quality and Safety, and a range of state and territory regulators and complaints bodies.

Health funds want privacy law reforms to provide clarity, so that they can be confidently implemented. Any efforts to consolidate and remove overlapping requirements would be welcomed by health funds.

Given the extensive range of proposed amendments and the need to adapt IT infrastructure to enable compliance with new obligations (such as the proposed new individual rights), there should be a reasonable transition period before the amendments take effect. When similar legislation was enacted across the European Union, it took several years for organisations to be in a position to comply with the General Data Protection Regulation (GDPR).

We have set out our detailed responses to the proposals below.

Response to the proposals

Proposals 4.1-4.6– definition of personal information

The proposed amendment to the definition of personal information (and sensitive information) would capture a broader range of information as a result of the change to the definition to 'relate to' individuals (including information created, deduced or inferred by an entity about a reasonably identifiable individual). Funds would welcome clear guidance from the Office of the Australian Information Commission (OAIC) about how the Australian Privacy Principles (APPs) will apply to the broader set of information that would be captured within the ambit of 'personal information'.

The proposed change to this definition will have a significant impact on businesses, including health funds. They will need to undertake costly technology and data governance process and policy reviews to ensure that their APP compliance processes apply not only to information about an individual, but also to information inferred or related to an individual, or information that is created or deduced by the entity or its contractors. As an example, the Funds would welcome clear guidance on what the expansion of this definition might mean in relation to information deduced or inferred from:

- lifestyle habits
- occupation and income
- age and life stage
- geographic location, and
- claims history.

Proposals 4.5 and 4.6 – de-identification of information

Health funds would welcome clarity and specific requirements regarding holding de-identified information to ensure that the information remains de-identified, including the factors that will be deemed sufficient to ensure an individual is not 'reasonably identifiable' on an ongoing basis.

In light of developing technologies, information that is de-identified at one point in time could become identifiable as new technologies can be applied to that information. The cost of applying new measures to ensure information remains de-identified can add significant costs to business operations. Therefore, the Funds query whether the intention is that entities will be required to periodically (eg annually) test de-identified information and technologies applied against latest technology, to ensure that the information remains in a state that cannot be re-identified using that technology.

Further, funds would welcome specific direction in regulations or guidance from the OAIC in relation to what are 'reasonable measures' to ensure third parties who receive de-identified information comply with the APPs, to ensure consistency in the industry, proper compliance with regulator expectations, and efficacy in their engagement and management of contractors.

Proposal 5.2 – temporary code making powers

The Report proposes to introduce powers for the Information Commissioner to issue a temporary APP code for a maximum of 12 months on the direction or approval of the Attorney-General if it is urgently required and where there is a public interest to do so.

Health funds generally support the intention of this proposal, but want to ensure the circumstances in which these APP codes are issued and the permitted scope of code changes are appropriately limited, as they will not be subject to consultation.

Similarly to New Zealand, the temporary APP code making powers should only operate after a state of emergency or national emergency has been declared.

Proposal 11.1 – amended definition of consent

PHA supports amending the definition of consent, to ensure that individuals have appropriate capacity, and are appropriately informed, before providing consent.

Guidance with respect to electronic medical devices would be welcomed. For example, many modern cardiac devices (and similar implanted electronic medical devices) collect patient information which is then owned by the medical device manufacturer. Many of these multinational companies keep these data in other countries, and may provide information back to the patient or their clinician. However, few patients understand this process. Where consent is obtained, it is bundled with consent for surgery, and information is provided at a time of significant distress for the patient.

Health funds would also like to ensure that the entities with pre-existing personal information, and pre-existing consents collected with respect to those consents, should be able to continue relying on the legacy consent with this new definition of consent applying to the new instances of consent and subsequent data collection.

Proposals 12.1 - 12.3 – fair and reasonable test

Health funds do not see the introduction of an objective 'fair and reasonable' test to their collection or use and disclosure activities as necessary. This test applies another overlay to existing rules for the handling of personal information and will likely add further uncertainty to the lawful handling of personal information.

Proposal 13.1 – privacy impact assessments (PIAs)

Funds already undertake PIAs as a privacy-enhancing process and note almost all of their activities would be considered 'high risk activities' and would require a PIA to be undertaken.

Funds would also welcome further guidance on what constitutes a 'high privacy risk activity', and specifically, guidance as to what constitutes a 'significant impact' to an individual within the context of their business as usual activities.

Given there are currently significant variations in the scale, range and comprehensiveness of PIAs, minimum requirements for PIAs should be codified in regulation. This would help clarify the depth of assessment required in particularly circumstances –particularly where an entity's primary business involves the collection and use of personal information on a large scale.

Proposal 14.1 – research

There is public benefit in health funds being able to conduct research using personal information, and PHA supports the proposal to include a legislative provision that permits broad consents for research purposes.

Proposal 15.1 – organisational accountability

The requirement for an entity to record the purposes for which it will collect, use and disclose personal information, including secondary purposes, is likely to be administratively burdensome. This obligation should include a defined scope as well as appropriate limitations.

Proposal 18.1 – additional rights: information about what an entity has done with personal information

Health funds would welcome clear guidance on the level of detail required for an entity to satisfy this obligation. A comprehensive history of how data fields have been used is likely to require expensive and complex information tracking, mapping and recording. A general register in relation to the various uses and discloses or transfer of information would appropriately balance transparency with being operationally practical.

Proposal 18.1(b) – additional rights: identifying the source of personal information

The burden and costs of requiring APP entities to maintain a record of the source of all personal information that they collect indirectly would be significant. For a health fund, keeping records of where all personal information has been collected and connecting that to either the information or the relevant person presents a significant information collection, management and security burden.

The funds accept that APP 7.6(e) currently includes a requirement for organisations to identify the source of personal information used in connection with direct marketing activities. However, APP 7.7(b) includes an exemption for organisations to comply with such a request if it is impracticable or unreasonable to do so. Proposal 18.1(b) does not include an equivalent exemption.

Further, the justification for including this proposal in the Report is based on equivalent laws in other jurisdictions. However, none of the examples given appear to bear this out. In particular:

- the GDPR only requires information about the source to be provided if it is available
- in Canada, such disclosure is 'encouraged'
- in Japan there is no equivalent
- in Singapore there is no equivalent, and
- in California, only the categories of sources need to be provided.

It's unclear how recommendation 18.1(b) as proposed provides greater consumer benefit than a general register outlining the aggregate sources of personal information collected by fund.

Proposal 18.3 – additional rights: 'erasure'

There are a range of existing laws, including the common law, that require health funds to retain information. Funds would welcome further guidance on the interaction between the proposed right of erasure, and the Funds' express or implied record retention obligations under existing legislation, such as:

- record keeping obligations under State and Territory health records laws, including minimum retention periods under those laws (which is seven years or until the individual is 25 years old)
- corporations and tax laws, and
- workplace relations laws.

PHA notes there is substantial public benefit in health funds maintaining health records – for example, health fund records were essential in identifying women who had received pelvic mesh implants when it became clear these medical devices were a risk to women's health. The providers of the material did not have comprehensive records, and records held by health providers (including doctors and hospitals) did not identify all the women affected. Health funds have proven to be longer lasting and more stable than individual medical businesses and many hospitals, meaning that records held by health funds are more complete.

It should be noted that in the European Union, there were some practical difficulties with successfully implementing this right as part of the GDPR. For example, where a request was received but not actioned due to competing legal requirements, continued retention of the information did not meet individual or community expectations.

Proposals 19.1 – 19.3 – automated decision-making

The report proposes the introduction of a right for individuals to request meaningful information about how substantially automated decisions with legal or similar effect are made. APP entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similar effect.

Funds use substantially automated decision-making processes to assess and process private health insurance claims. The use of these tools helps to lower the cost of private health insurance for Australians and are a large part of the reason management expenses for private health insurance are many orders of magnitude lower than for other types of insurance. Funds invest heavily in systems to lower the costs of processing claims for their members.

Information about funds' systems is commercially sensitive, and it would be detrimental to their businesses if this were made publicly available. Any amendments should not intrude on a fund's ability to make commercially confidential decisions or engage in product development or service automation.

Funds' systems are already subject to internal and external audits to ensure they meet applicable legislative and regulatory requirements. Further, there are existing complaints mechanisms in place (both internally and externally through the Private Health Insurance Ombudsman) that are available to members who wish to complain about decisions.

Therefore, PHA submits that the detriment to APP entities in being compelled to reveal specific commercially sensitive information and processes about their automated decision-making is not warranted by any commensurate benefit to individuals, and should not proceed.

However, general information about the use of automated decision-making should be included in an entities' public-facing statement on AI or in other policy documents, such as their privacy policy, to ensure consumers understand the general nature of how funds use automated decision making.

Proposals 20.5 and 20.8 – regulation of targeted advertising

There is significant public benefit in targeted health promotion activity, and this is core business for health funds. It is important that the proposals for regulation of targeted advertising provide for a wide definition of health promotion activities.

Around half of Australians live with a chronic health condition, and chronic diseases cause 9 out of every 10 preventable deaths and account for 85% of years lost due to ill health or early death.[1] There is a clear public benefit in providing general and targeted health information.

Using healthcare data to proactively look after people's health outside of hospital is a critical direction of the healthcare sector. This is true for both public and private systems of Australia, as well as globally. This is because using health information to help a patient before their health deteriorates reduces their chance of an emergency hospital admission and associated morbidity and mortality.

There are a number of programs across the sector to support patients outside of hospital that have significant impacts to Australians health experience, outcomes and quality of life. Most programs use health data to identify the most vulnerable patients to support with more health coordination, which has led to a substantial reduction in hospital admissions within this cohort for target conditions, and significantly greater survival rates for chronic conditions such as cancer and heart disease.

[1] See https://preventioncentre.org.au/about-prevention/what-is-the-burden-of-chronic-disease/

There is a risk that privacy constraints designed to stop companies using customers' personal health data for profit could unintentionally hinder these vital services for Australians. That could also lead to significantly increased morbidity and mortality if the sector is constrained in its ability to contact customers for these purposes.

The *National Health Prevention Strategy 2021-2030* highlights the importance of health promotion and highlights private health funds as having an important role in prevention. All health funds provide general information about healthy lifestyles and targeting information on a range of topics, such as vaccination, screening, self-care, mental health, particular risk factors and services that may help members avoid death and disease.

In addition to general points around health promotion, the proposals to limit targeted advertising to children requires a more nuanced response. Children, in particular older children, are recognised through the common law and state and territory legislation as being capable of making health decisions, with promotion of sensitive areas such as sexual health, eating disorders and mental health care being much more effective when delivered directly rather than relying on parents and guardians.

Health funds have a strong vested interest in promoting good health, as it provides benefits to the community, governments and their own businesses, in addition to the benefit to the individual. Health promotion should be encouraged by changes to the Privacy Act.

Proposal 20.9 – providing information about algorithms

Similar to proposal 19.3, the additional burden of disclosing algorithm and profiling information may be prohibitive and reveal commercially sensitive information. This would be a disincentive to improve services to members and may ultimately lead to detrimental public health outcomes.

A more general public statement on the use of algorithms would provide the vast majority of the benefits of the proposal and ensure consumers understand the general nature of how funds use automated decision making for marketing and health promotion activities.

Proposal 21.6 – retention periods

Funds are supportive of the proposal to undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with relevant privacy and cyber security risks.

In addition, funds would support increased clarity as to when an organisation can destroy or de-identify personal information, particularly in light of the various overlapping retention and destruction obligations under Commonwealth, State and Territory legislation and the common law.

Proposal 23.2 – prescribing countries and certification schemes

It would be useful to understand whether it is intended that the 'whitelist jurisdictions', prescribed certification scheme(s), and standard contractual clauses, will reflect those already identified and created in the European Union as part of GDPR, or whether these will be tailored to Australian and Asia Pacific markets.

Proposal 27.1 – statutory right for serious invasions of privacy

Further guidance on what constitutes 'serious' in the context of this proposal is required.

Proposal 28.1 – multiple reporting obligations

Health funds have reporting obligations under multiple notification frameworks. Clarity is needed on the harmonisation and intersection between the various regulatory security and data incident reporting obligations, which includes Prudential Standard CPS 234, the security of critical infrastructure laws, and the notifiable data breach regime under the Privacy Act.

Funds would also welcome an understanding from the OAIC, the Australian Prudential Regulation Authority, and the Cyber and Infrastructure Security Centre, about how they intend to efficiently and effectively regulate the intersection between each of these laws.