Avant
By doctors for doctors

Avant Mutual Group Limited
ABN 58 123 154 898

Registered office
Level 6, Darling Park 3
201 Sussex Street, Sydney NSW 2000

Postal address
PO Box 746 Queen Victoria Building
Sydney NSW 1230

DX 11583 Sydney Downtown

avant.org.au

Telephone 02 9260 9000 **Fax** 02 9261 2921
Freecall 1800 128 268 **Freefax** 1800 228 268

31 March 2023

Privacy Act Review
Attorney-General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

By email: PrivacyActReview@ag.gov.au

Government response to the Privacy Act Review Report

Thank you for the opportunity to comment on the Privacy Act Review Report.

Avant is the largest medical defence organisation in Australia. We provide professional indemnity insurance and legal advice and assistance to more than 82,000 medical practitioners and students around Australia.

Our submission is attached.

Yours sincerely

Georgie Haysom
General Manager, Advocacy, Education and Research
Email: georgie.haysom@avant.org.au

Avant Mutual Group Limited
ABN 58 123 154 898

Avant submission on the Privacy Act Review Report

Avant is a member-owned doctors' organisation and Australia's largest medical indemnity insurer, committed to supporting a sustainable health system that provides quality care to the Australian community. Avant provides professional indemnity insurance and offers legal advice and assistance to more than 82,000 healthcare practitioners and students around Australia (more than half of Australia's doctors). Our members are from all medical specialities and career stages and from every state and territory in Australia.

We assist members in civil litigation, professional conduct matters, coronial matters and a range of other matters. Our Medico-legal Advisory Service provides support and advice to members and insured medical practices when they encounter medico-legal issues. We aim to promote quality, safety and professionalism in medical practice through advocacy, research and medico-legal education. Privacy is a key area for medico-legal advice and education.

We support retaining the principles-based approach of the Act. Given that approach, we support the important role that the OAIC plays in publishing clear guidance documents to explain the operation of the privacy legislation and its practical implications. Some specific areas where this would be useful include:

- the introduction of standardised templates and layouts (section 10);
- understanding the 'fair and reasonable' principle and proportionality (section 12);
- the implementation of additional protections, especially the Privacy Impact Assessment process (section 13);
- organisational accountability (section 15);
- amendments to the existing guidance regarding children and capacity to consent (section 16); and
- clarification regarding the factors to be considered when exercising enforcement powers under section 13G (section 25).

We would welcome the opportunity to work with the OAIC in relation to these.

We agree that proposals that have not had the benefit of stakeholder feedback will require further consultation before implementation.

Many of these changes are significant and it is important that there be sufficient time for entities to ensure compliance. This will include updating their current privacy material including privacy notices and their privacy and other policies and procedures, and training staff.

We have made previous submissions to the consultations on the Issues Paper and Discussion Paper. We have referred to those submissions below where relevant. In this submission, we have commented on some but not all of the proposals and have adopted the numbering of the section and respective proposals in the Privacy Act Review Report ("the Report") to reference our comments.

General comments

We noted in our previous submissions that the review has not included consideration of either the permitted general situations or the permitted health situations under sections 16A and section 16B of the *Privacy Act* at all. In our view, these generally work well but there are some nuances with the wording of some of the provisions that could be clarified to strengthen the protections under the Act. For example, provision of a patient's medical records to a complaints body may not squarely fit within the exemptions under the Act. Avant would welcome the opportunity to be involved in further consultation regarding the operation of these sections.

4.6. Information about deceased individuals

We note from the Report that the Standing Council of Attorneys-General plans to develop uniform model legislation for a national access scheme for digital records after death or incapacity. We assume this would apply to the electronic medical records of deceased patients. We recommend that this be extended to ensure it also applies to all medical records for deceased patients, not only digital records. The reasons for this were set out in our submission to the Issues Paper and Discussion Paper.

7. Employee records exemption

As stated in our submission to the Discussion Paper, Avant supports extending privacy protections to private sector employees as outlined in Proposal 7.1. We agree that further consultation would be needed on how privacy and workplace laws should interact.

10. Privacy policies and collection notices

We agree with Proposal 10.3 regarding the use of standardised templates. Many healthcare service providers are small businesses and there is a significant compliance burden. Having standardised terminology and icons where appropriate would also benefit patient understanding.

At the same time, as we say in our medico-legal education to doctors, consent is a process not a form. Merely providing a standardised consent form and asking the patient to accept it does not mean that consent is informed or that the patient has understood the information provided.

It would therefore be important to ensure that any standardised templates are tailored to specific sectors and that they are flexible enough to be adapted to local situations. Any templates should also comply with any relevant accreditation standards (for example, General Practice accreditation standards).

We strongly support the proposal that OAIC guidance be used to support the introduction of standardised templates and layouts, as this would assist with clarity.

12. Fair and reasonable personal information handling

We support the approach in Proposal 12.1 and the framework outlined in Proposal 12.2. This will be of benefit for healthcare providers when considering and responding to issues regarding the collection, use or disclosure of sensitive health information.

In particular, we consider that it could be useful in "filling the gap" that exists in guidance in some areas, such as in relation to managing issues regarding the disclosure of deceased patient records (see comments above regarding section 4.6 regarding deceased patient medical patients). This is a common issue for health practitioners and practices, compounded by the inconsistency or absence of frameworks across state and territory jurisdictions.

We consider that in addition to noting relevant considerations for determining 'proportionality' being in the EM, there should be additional guidance from the OAIC.

13. Additional protections

We understand the rationale behind Proposal 13.1. However, in the context of the provision of healthcare, we are concerned about the implementation of the proposal that all entities covered by the Act should conduct a Privacy Impact Assessment (PIA) before commencing an activity which is likely to have a significant impact on the privacy of individuals.

Almost everything a health care provider or practice does relates to sensitive information, and most, if not all, activities are likely to have a significant impact on the privacy of individuals. Healthcare providers and practices will need a great deal of guidance and support to undertake a PIA, and many may not have the resources either to outsource or conduct the PIA themselves.

It would be helpful if the OAIC could develop guidance to assist entities to conduct PIAs, or limit the activities for which PIAs are required. This could be done by way of appropriate exemptions for specific sectors or limited to certain activities for those sectors.

We support Proposal 13.3 as guidance from the OAIC is particularly helpful in supporting healthcare professionals and practices understand their obligations as new situations emerge.

In relation to Proposal 13.4, we agree that OAIC guidance should supplement this proposal to provide clarity regarding what reasonable steps, if any, would be required in different situations. This applies both in relation to our members and in Avant's corporate context, as outlined in our submission to the Discussion Paper.

14. Research

Concerns about privacy can sometimes be seen as a barrier to research that may be otherwise beneficial to the public good. Avant supports the approach outlined in Proposals 14.1 to 14.3, in particular permitting *broad consent* for the purposes of research. We agree that consideration should be given to broadening the scope of research permitted without consent, and developing a single exception and a single set of guidelines, and that further consultation is required on these proposals.

15. Organisational Accountability

It is currently unclear how Proposals 15.1 and 15.2 would apply in a healthcare context. We are concerned about the potential administrative burden on healthcare providers and practices of these proposed obligations. Further specific guidance from the OAIC would be required to assist with implementation and we would welcome the opportunity to be involved in developing this guidance.

16. Children

We are pleased to see that the capacity of children to consent to information handling is to be determined on a case by case basis, which is consistent with the common law.

We confirm the position outlined in our submissions to the Discussion Paper and Issues Paper, being that it is important that APP entities in healthcare should be permitted to assess capacity to consent on an individualised basis, where appropriate, as they do currently in relation to healthcare decisions. This would apply to exercising other privacy requests including access, correction, objection or erasure.

Whilst we agree in principle that the OAIC guidance should continue to be relied on, it would benefit from review and revision. Our ongoing concern is the potential for confusion where entities rely on the presumption of a lack of capacity under the age of 15 and release information where it is not in the best interests of the child. The exceptions outlined in Proposal 16.2 should be clearly stated in amendments to the OAIC guidance. This is particularly important given that other legislation refers to 14 as the age of presumed capacity.[1]

17. People experiencing vulnerability

We support the principles underpinning Proposals 17.1 and 17.2.

Any guidance from the OAIC as referred to in Proposal 17.2 would also need to consider and ensure consistency with the legislative position in each state and territory and any current Commonwealth legislation. This would be an appropriate issue for the

[1] Such as the *My Health Records Act 2012* (Cth), and the *Minors (Property and Contracts) Act 1970* (NSW).

Commonwealth, State and Territory working group to consider, to ensure harmonisation of privacy laws as per Proposal 29.3.

18. Rights of the Individual

The practical implications of the proposals in this section are concerning in a healthcare context, as allowing these rights without qualification or exception could impact on healthcare delivery. Therefore we agree with the comment (in relation to competing public interests) that consideration should be given to applying health care and research exceptions to these rights.[2] In our view, there should be a general exception for all rights of the individual in the public interest for health information, beyond the specific exceptions in section 16B of the Act.

We provide comments in relation to several of the proposals below.

Proposal 18.1(b)
We are concerned about how this will apply to confidential unsolicited information. Sometimes doctors receive information from patients' family members relevant to the patient's care (which must be documented and retained in compliance with their professional and legal obligations). Revealing the source of the information may pose a risk to the patient's ongoing care and their health and safety. It would be important that this provision was subject to the existing disclosure exception regarding serious risk to life, health or safety.

Proposal 18.3
We confirm the position set out in Avant's submission to the Issues Paper and Discussion Paper that any right of erasure should not apply to healthcare entities.

Proposal 18.5
We support the introduction of a right to de-index online search results, as this may assist in minimising the reputational damage that may be caused by search results.

Proposal 18.6
We support this proposal to introduce exemptions to all rights of the individual based on the categories listed. As noted above we agree that consideration should be given to a general exemption for healthcare in the public interest.

Proposals 18.7, 18.8 and 18.9
These proposals should be read subject to the general exemptions. For example, if healthcare is exempt from these rights, there would need to be clarity about whether healthcare practitioners and practices were required to notify individual that these rights did not apply, and the consequences of that.

[2] Page 181 of section 18.8.1 of the Privacy Act Review Report.

21. Security, retention and destruction

We agree with Proposals 21.3, 21.5 and 21.6.

In relation to Proposal 21.7, we note that in the Australian Capital Territory, New South Wales and Victoria, there are already legislative obligations regarding retention of medical records. However, there is no legislation in place in the other states and territories and therefore no existing legal framework. Proposal 21.7 has the potential to cause confusion and inconsistency regarding retention of medical records in those jurisdictions. This is an area that would benefit from national consistency and harmonisation of laws regarding retention of medical records and would be an appropriate issue for the Commonwealth, State and Territory working group to consider as per Proposal 29.3.

23. Overseas data flows

We strongly support these proposals, for the reasons outlined in our submissions to the Issues Paper and Discussion Paper.

25. Enforcement

We are concerned that the addition of civil penalties for interferences of privacy that are not serious or repeated will lead to increased litigation costs and significant administrative burden. In our view, the proposed low-level penalties outlined in Proposal 25.1 are not proportionate to the risk posed by any non-compliance. In our experience, any non-compliance in this area would be innocent and inadvertent and an educative approach to compliance is to be preferred.

We agree with the principle underpinning Proposal 25.2 to clarify what is a serious interference with privacy. Whilst we agreed in our submission to the Discussion Paper that the legislation could more clearly capture beaches involving “highly sensitive information” we note that Proposal 25.2 refers to “sensitive information or information of a sensitive nature”. This is a much broader category and would apply to all health information. The wording of any clarification of section 13G would need careful consideration to ensure it is reasonable and proportionate.

We agree that the OAIC will need to provide further specific guidance about the factors that it will take into account when determining whether to take action under section 13G.

In relation to Proposal 25.7, we agree further work would need to be done regarding any industry funding proposal. There is increasing concern about the sustainability of Australia’s healthcare system and in particular, primary care. An industry funding proposal would potentially impose a significant financial burden on already stretched medical practices, many of which are small businesses, funded either partly or entirely through Medicare payments, and that deal with sensitive healthcare information on a daily basis.

In relation to Proposal 25.10, we are concerned about the OAIC having an increased focus on enforcement at the expense of its significant and helpful educative role. As stated above, in our experience, non-compliance is often inadvertent and easily rectified with a focus on education.

26. A direct right of action

As outlined in our submissions to the Issues Paper and Discussion Paper, we oppose the introduction of a direct right of action. In particular, we consider that the proposed threshold is too low, and would lead to increased legal costs and court costs and the risk of overinflated views of damages entitlements. Any direct right of action should be subject to a higher threshold of loss and damage beyond that which is currently in the Act, which includes injury to a person's feeling or humiliation.

We note the proposal that a direct right of action be available to individuals and representative classes of individuals. We are concerned about the potential for class actions under this right. We are seeing increasing class actions in the medical liability space and we would be concerned if this were to follow in the privacy space as a consequence of these reforms.

If a direct right of action were introduced, we strongly support gateway provisions including compulsory conciliation and leave of the court to proceed. Costs should follow the event as per the usual costs orders in the Federal Court.

27. A statutory tort for serious invasions of privacy

As set out in our submissions to the Issues Paper and Discussion Paper, we oppose this proposal and do not consider that a statutory tort of privacy is necessary particularly in the healthcare context. While we note the essential feature of the proposed cause of action as outlined in the ALRC Report 123 Model, it is not clear whether or how such a cause of action would apply in the healthcare context.

As with the direct right of action, our concern is that legislating a statutory tort of privacy will increase costs to the system via increased legal costs and court costs.

Nevertheless, we are pleased to see that if a statutory tort of privacy were to be introduced, it would only apply to intentional or reckless invasions of privacy, and would not extend to negligence or be based on strict liability. It should be clear what is to be covered under this tort, as compared with a direct right of action. There should be compulsory conciliation and other alternative dispute resolutions options and there should be a cap on any compensation awarded.

Consideration should also be given as to how this tort might align with other legislative regimes, such as state-based civil liability, surveillance devices and defamation legislation, particularly in terms of recovery of compensation and heads of damage. This would be an appropriate matter for consideration by the working group.

28. Notifiable data breaches scheme

We support Proposal 28.1 to facilitate greater understanding of and compliance with reporting obligations of entities.

We oppose Proposal 28.2 given the significant burden on medical practitioners and practices, as well as in Avant's own business operations. Reporting at that early time would also largely be ineffective given the lack of information that would be available, the complexities of data breaches and the challenge of obtaining relevant information within such a short period of time. While we recognise that the proposal allows for further information to be provided at a later time, this is not sufficient to warrant the 72-hour notification period. If the time period is to be reduced from the current 30 days, we recommend a period of 14 days would be more appropriate to enable collection and analysis of the necessary information to make the notification effective.

29. Interactions with other schemes

We strongly support Proposal 29.3 and the benefit to be achieved by harmonisation of privacy laws across Commonwealth, state and territory jurisdictions. As noted above, for consistency, we recommend that the working group consider harmonising laws with respect to the following issues:

- Deceased individuals' personal/health information.
- Supported decision-making (capacity and consent).
- Minimum retention periods for health care information/medical records.
- Alignment of the statutory tort of privacy (if it is to be enacted) with other legislative regimes, such as state-based civil liability, surveillance devices and defamation legislation.

Avant Mutual
31 March 2023