AUSTRALIAN MEDICAL ASSOCIATION
ABN 37 008 426 793
T | 61 2 6270 5400
F | 61 2 6270 5499
E | ama@ama.com.au
W | www.ama.com.au
39 Brisbane Ave Barton ACT 2600
PO Box 6090 Kingston ACT 2604

Privacy Act Review Report

AMA submission to the Attorney General's Department Consultation on the Government response to the Privacy Act Review Report

privacyactreview@ag.gov.au

The AMA thanks the Attorney General for the opportunity to submit to this consultation. AMA also acknowledges and welcomes that several of our responses to the October 2020 Issues Paper and the 2021 Discussion Paper have been accepted and acted on by the Attorney General's Department, specifically our suggestions around:

- **A child's capacity to consent**, particularly in healthcare situations, where it would be harmful to the child or contrary to their interests to require parental or guardian consent to collection, use and disclosure of their personal information; and enabling doctors to determine that a child under 15 has the capacity to consent to collection, use and disclosure of their personal information for the purposes of receiving healthcare.
- **Best interest of a child** - Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances; and
- **Health research**, such as broad consent for research purposes and further consultation on broadening the scope of research permitted under the Act, as well as single set of guidelines.

This submission will only address proposals that the AMA believes should be improved to ensure that the review does not inadvertently inhibit the delivery of health care.

Proposal 4.3 – Amend the definition of 'collection' to expressly cover inferred or generated information

The AMA still has concerns around this proposal and how it may impact medical professionals. As noted in our past submissions, doctors routinely infer sensitive information about their patients from other information (such as test results). As acknowledged in the Report (page 30):

> *A doctor forming an opinion about a patient's health ... would be sensitive information and require notification and consent under the APPs*

> *Collection of inferred and generated information occurs at the point of inference or generation. APP 5 would require notice (and, if applicable, consent) at the time of collection, or as soon as practicable afterwards.*

Accordingly, we continue to have concerns about the administrative costs of Proposal 4.3 for doctors, particularly GPs and other doctors operating private practices. If this amendment proceeds, the Explanatory Memorandum or other guidance should acknowledge the response provided in the Report to our concerns (also on page 30):

> *The steps to give notice or otherwise ensure the individual is aware of relevant matters are those steps that are reasonable in the circumstances (if any). If the inference made is a natural inference that the individual would expect or it is inseparable from the original information, for example a diagnosis that an individual has a disease from test results, then APP 5 notice would not likely be required.*

This issue also needs to be addressed in the context of APP 3 (proposal 11.1).

Proposal 4.4 – Establish non-exhaustive list of circumstances APP entities will be expected to have regard to in considering whether an individual is "reasonably identifiable"

The Discussion Paper proposed expanding the definition of "personal information" to state that:

> *"an individual is reasonably identifiable if they are capable of being identified, directly or indirectly."*

This amendment was questioned by the AMA in our submission and we are pleased that the Review is no longer considering it. We are also pleased that the Report acknowledges (on page 37) that:

> *Given the impracticality of achieving irreversible anonymisation, a complete anonymisation standard is not warranted in the Privacy Act.*
>
> *APP entities may be able to engage in 'functional de-identification' with strict organisational and technical controls so that identifying information is separated. This enables risk managed use, even though without the controls the information would be personal information.*
>
> *De-identification is different to true anonymisation which may only be achievable by aggregating individuals' data together.*

However, the Report continues to propose (Proposal 4.4) that:

> *'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.*

The Report suggests (on page 35) that:

The circumstances to aid assessment of reasonable identifiability, could include:

- *the nature and volume of the information*
- *who holds or has access to the information*
- *how and why the information is collected, used, stored and disclosed*
- *the other information that is available (or known) to the recipient, and the practicability of using that information to identify an individual, and*
- *the context in which information is handled, including the context into which information will be disclosed.*

It is unclear whether this list is intended to be statutory or in a guidance document issued by the OAIC. It is also unclear (from the words "will be expected") whether compliance is mandatory or encouraged and, in either case, what form of records must be kept by APP entities to show that they have considered each item on the list. The Review states (on page 34) that:

> *The OAIC considered that any list should remain in OAIC guidance rather than being in the Act; with the OAIC recommending that APP entities should be required to have regard to their guidance.*

As noted in our submission to the Discussion Paper (page 3), our primary concern relates to the disclosure of de-identified patient information for the Practice Improvement Program. Few GP practices will have the resources (or access to the information) required to apply this list. Depending on the drafting, this concern may be addressed by the proposed research exception (Proposal 14).

Proposal 4.5 – Amend the definition of "de-identified" to refer to "best available practice"

The Report also proposes that the government:

> *Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information that involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.*

The Report contains very little further detail about Proposal 4.5. In particular, it is unclear whether APP entities are required to apply "best available practice" and, if so:

- how APP entities (particularly small businesses such as GP practices) will know what "best available practice" is?
- how regularly an APP entity is required to consider whether or not their de-identification policies comply with "best available practice".

It is also important to consider the consequences of past disclosures if there is a change in the de-identification standard. One option would for the recipient to be required to apply additional

processes to the data held by them to meet the new standard (i.e., such that it would continue to be de-identified). Treating the information as if it is "personal information" (either retrospectively or prospectively) may impose unrealistic obligations on both the discloser and the recipient. For example, the recipient will not have sufficient information to issue APP 5 notices in relation to the "collection". Similarly, it may be unrealistic for the discloser to go back and get consents to disclosure from the affected individuals.

Our concerns about these practical issues (particularly for practitioners who disclose de-identified patient data for research and quality improvement purposes), is prompted by the following paragraphs (on page 37):

> *[D]e-identification should not be viewed as a static condition.*
>
> *De-identified information for the purposes of the principles-based Privacy Act should be defined to make it clear that de-identifying information is a process that involves treating it in such a way so as to not allow an individual to be reasonably identifiable while those circumstances persist.*
>
> *The current definition in section 6 of the Act and in the APPs speaks of de-identification in the present tense, as a task that could be performed and 'de-identification' achieved. However, de-identification is subject to its circumstances. When those circumstances change (for example it is moved to a new environment or new linkable information is introduced), an APP entity cannot rely on the past de-identification and must conduct a proportional reassessment and possibly further de-identification.*

The AMA acknowledges that the Report invokes the flexibility of the Privacy Act to develop codes, to assist when further standards and guidance are required due to technically complex and evolving uses (page 37). This is preferable to imposing uncertain standards such as "best available practice" on what are predominantly small businesses.

Proposal 4.6 – Extend APP 11.1 to de-identified information

We note also that, whether or not the information meets the standard for "deidentified" information at a point in time, under new Proposal 4.6 the recipient would need to:

> *take such steps as are reasonable in the circumstances to protect [the] information:*
> *(a) from misuse, interference and loss; and*
> *(b) from unauthorised re-identification, access, modification or disclosure.*

In our view, this Proposal is more practical than Proposal 4.5 in that it requires APP entities that hold information:

- to continuously consider whether that information is appropriately secured; but

- does not require them to retrospectively comply with provisions (particularly APP 3 and APP 5) that apply to identifiable information.

Proposal 5.5 – Permit organisations to disclose personal information to State and Territory authorities (other than SA and WA) under an "Emergency Declaration"

As noted in our submission to the Discussion Paper, the AMA is not supportive of the proposal to amend the Act to permit organisations to disclose personal information to State and Territory authorities when an Emergency Declaration is in force, for a permitted purpose.

The Report proposes (Proposal 5.5) that the government:

> *"Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth."*

The Report does not set out which States and Territories meet this test. We assume it is intended to allow disclosure to all State and Territories except Western Australia and South Australia. (https://www.oaic.gov.au/privacy/privacy-in-your-state) This should be clarified, particularly given that the Report is proposing amendments to the Privacy Act that may not be enacted by other jurisdictions.

The AMA shares the concerns of other agencies, as reported in the Report, that ED provisions do not limit disclosure to specific information sharing acts or practices for particular types of entities. We are in favour of a narrower scope of information sharing under EDs where appropriate, in order to achieve better balance between privacy protections and sharing of personal information (page 50). This is consistent with the proposal (Proposal 5.3) that the government:

> *Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to:*
> - *entities, or classes of entity*
> - *classes of personal information, and*
> - *acts and practices, or types of acts and practices.*

As noted in our submission to the Discussion Paper, while COVID-19 has been provided as justification for increased sharing of data without patient consent, no emergency declaration was actually made under Part VIA in relation to the COVID-19 pandemic. The AMA maintains this position.

Proposal 10 – Privacy policies and collection notices

The Discussion Paper made multiple proposals that would expand the circumstance where APP entities were required to issues APP 5 notices. In our submission, we expressed concern about how these proposals would achieve the objectives of obtaining genuine consent without

overloading consumers with unnecessary notifications, particularly in the context of medical care and medical professionals engaging with patients.

The Report proposes that (Proposal 10.1) that APP 5 be amended to:

> *Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise, and understandable.*

The Report notes (on page 96) that the term “up-to-date" was selected (rather than “current”) to:

- achieve greater alignment with the existing requirements of APP 1.3; and
- more clearly convey the intention that collection notices procedures would only need to be updated when practices change.

We support this approach.

The Report also proposes that (Proposal 10.3) that:

> *Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.*

We welcome any Proposals that aim to provide clarity around what information should be included in the APP 5 collection notice, including development of templates for particular sectors, including the health sector. The guide produced by OAIC for the health sector has been a valuable resource. Given that doctors predominantly practice through small and medium enterprises, appropriate time and resources should be provided for transition to any mandatory requirements (such as new APP Codes).

We have concerns about Proposal 10.2. It recommends that the following new matters be included in an APP 5 collection notice:

> *(a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure*
> *(b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and*
> *(c) the types of personal information that may be disclosed to overseas recipients.*

As discussed further below (in relation to Proposals 13 and 17.1), all hospitals and medical practices may fall within the proposed definition of “a high privacy risk activity”. It is unclear from

the Report (particularly the explanation on page 98) whether practices would be required to use the words "high privacy risk activity" in their APP 5 notices or they would simply notify (as is the case now) that they collect, use and disclose patient information in order to provide medical services.

There is also very little explanation in the Report as to what a medical practice would need to do to comply with new paragraph (b). Proposal 18.7 is that:

> *Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them.*
>
> *Privacy policies should set out the APP entity's procedures for responding to the rights of the individual.*

In relation to this proposal, page 183 of the Report states that:

> *Entities are currently required to notify individuals at the point of collection that the privacy policy of the APP entity contains information on how to access and seek correction of their personal information. It would be appropriate to extend that obligation to all the rights of the individual. Privacy policies should include relevant information on its procedures for responding to the rights of the individual.*

Based on the summary by Proposal 18 on page 11, our understanding is that these Proposals would require APP entities (including all GPs and other medical practices) to include the following additional information in APP 5 notices (in addition to alerting them to their existing rights under APP 12 and APP 13):

- The patient's right to require the doctor to identify the source of any information collected from a third party.
- The patient's right to require the doctor to provide for a nominal fee "an explanation or summary of what it has done with [their] personal information".
- The patient's right to object to use or disclosure of their personal information.
- The patient's right to have their personal information erased.

It is unclear from the Review whether all APP entities would be required to notify individuals of:

- their right to de-index online search results containing personal information (Proposal 18.5); or
- the proposed direct right of action (Proposal 26.1).

As discussed further below, the AMA continues to have concerns about the cost and practicality of some of these new rights, particularly in the context of GPs and other small medical practices.

The AMA welcomes the proposal (Proposal 10.3) that there be standard templates and layouts for privacy policies and collection notices, with standardised terminology and icons for relevant sectors. We would like to see a standard template developed for the health sector.

We would also welcome guidance that makes it clear that that new paragraph (c) is not intended to require doctors to notify patients that they use medical software or storage systems that utilise cloud services. This is consistent with Proposal 23.6. By contrast, a provider would be required to inform users if it is hosted overseas (e.g. a health app or telehealth provider) or sells data about users (e.g. a script service) to third parties located overseas.

Proposal 11.1 - Require that consent be current and specific

Proposal 11.1 recommends that the government:

> *Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous*.

The Report contains the following commentary (on page 104) about healthcare settings:

> *The OAIC observed that implied consent is important in the healthcare context, for example, 'where a medical practitioner collects a specimen to send to a pathology laboratory for testing, it can be implied from the conduct of the individual that they consent to the laboratory collecting their health information, without the need for the laboratory to seek further express consent from the individual'...*
>
> *[The] reference to 'clear action' [proposed in the Discussion Paper] should not be included in the proposed definition of consent so that implied consent may continue to be relied upon in these limited circumstances. However, an entity that wishes to rely on implied consent would still be required to demonstrate that the implied consent was 'unambiguous'. This would continue to allow for implied consent in the clinical healthcare context, while restricting the use of implied consent in commercial settings where there is ambiguity as to the consumer's intention or knowledge as to how information is proposed to be handled.*

While the AMA supports these observations, doctors will still need guidance about what Proposal 11.1 requires in practice. For example, when a patient visits their GP, do they need to expressly consent to their records being provided to:

- Other GPs at practice (including locums)
- Other specialists (as part of a referral)
- Administrative staff
- Billing agencies and debt collectors
- Medicare
- Third parties who take over the practice or its records (as part of a sale or closure)

- PSR and Ahpra
- Medical Defence Organisations/ legal advisers
- Primary Health Network (as part of research and practice improvement)?

As noted above, for Proposal 10.1, the term “up-to-date" was selected (rather than “current”) to:

- achieve greater alignment with the existing requirements of APP 1.3; and
- more clearly convey the intention that collection notices procedures would only need to be updated when practices change.

These considerations are also relevant to “consent”. The AMA wants clarity that “current” does not require that practices send out letters to patients at regular intervals (e.g. 12 months) to confirm they still consent to their personal information being used and collected.

Proposal 11.3 - Make it easier to withdraw consent

Proposal 11.3 recommends that the government amend the Privacy Act to:

> *Expressly recognise the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent would not affect the lawfulness of how the personal information was handled before the consent was withdrawn.*

As noted in our previous submission, there are areas where it is feasible for a patient to ”opt out” of a particular use or disclosure of their health information. For example, a patient is entitled to:

- delete their My Health Record, change access controls for their My Health Record or tell their doctor not to record some types of information to My Health Record in the future;
- tell their specialist to stop sending updates to their referring GP; or
- tell their GP that they no longer want to be treated by them.

However, the patient’s right to withdraw consent should not trump the doctor’s rights to use and disclose the doctor’s existing records. These records are generally owned by the practice and are separate to the records held on My Health Record.

Proposal 11.3 states that the withdrawal of consent “would not affect the lawfulness of how the personal information **was handled before** the consent was withdrawn”. This emphasises that previous collections will not be retrospectively unlawful. However, any future uses or disclosure would have to be rely on exceptions that do not require patient consent. The Report states (on page 107) that:

> *Withdrawal of consent would not be subject to the exceptions to the Rights of the Individual. Consent is already subject to the general exceptions to the APPs. These exceptions would also apply where withdrawal of consent may not be possible or would be contrary to other public interests (such as research and medical services).*

It is not clear to the AMA what exceptions are being referred to here. While there are some specific exceptions for health information in section 16B, only item 4 (use or disclosure of genetic information to a genetic relative) would allow a doctor to disclose a former patient's health records and it only applies where use or disclosure is "necessary to lessen or prevent a serious threat to the life, health or safety". This means that doctors would need to rely on generally applicable exceptions.

For example, use or disclosure is permitted (without consent) where:

- required or authorised by law (APP 6.2(b))
- reasonably necessary for the establishment, exercise or defence of a legal or equitable claim (Item 4 of section 16A) or for the purposes of a confidential alternative dispute resolution process (Item 5 of section 16A)

These exceptions will apply where:

- a former patient sues (or threatens to sue) a doctor;
- a doctor is forced to commence (or threaten to commence) debt recovery proceedings against the patient; or
- a court or a government body (such as Ahpra, the Medical Board, Medicare or Professional Services Review) requires the practice to produce the records.

However, it is less clear how these exceptions apply where there is no "claim" or a government agency does not issue a formal notice to produce. For example, a doctor may provide information about their practice to their insurer as part of negotiating premiums. It is also common for regulators to issue "Please explain" letters prior to any formal claim or notice to produce. OAIC also refers (in Chapter 3 of their guide for health practitioners[1]) to a quality auditor examining patient records 'on the spot'. OAIC treats normal business practices as being within the patient's reasonable expectations and hence not requiring express consent. APP 6.2(a) allows use or disclosure where:

> *the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:*
>
> *(i) if the information is sensitive information--directly related to the primary purpose; or*
> *(ii) if the information is not sensitive information--related to the primary purpose.*

There is some existing case law to the effect that a person may "reasonably expect" disclosure even if they do not consent (and strongly object to) disclosure. These have included instances where personal information has been disclosed to debt collectors or published in response to

[1] Office of the Information Commissioner 2023. Privacy Guidance for organisations and government agencies. Guide to health privacy https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/guide-to-health-privacy

allegations. The AMA would welcome further guidance and clarification on how Proposal 11.3 (ability to withdraw consent) is intended to operate with APP 6.2(a) and, in particular, confirmation that withdrawal of consent does not (of itself) prevent practices from continuing to use information for normal business practices. (As discussed below, new Proposal 12 would still require that any use and disclosure under APP 6.2(a) would still be fair and reasonable.)

As noted in our previous submission, there may also be scenarios where pathology results, reminders or discharge practices for former patients are sent to the practice. APP 4.3 requires entities to **destroy or deidentify** any personal information that they receive that they could not have lawfully collected. If the patient has withdrawn their consent, collection will only be lawful if another exception applies. In this scenario, the "safest" course from a purely privacy perspective would be for the practice to destroy the new information. This approach is obviously problematic from a public health perspective.

If Proposal 11.3 (withdrawal of consent) is implemented, the AMA would welcome guidance as to whether existing exceptions would allow the practice to:

- phone the former patient (using contact details on file) to ask where they want the new information forwarded (and to keep a record of this interaction); or
- phone the source of the new information (without contacting the patient) to let them know the person is no longer a patient and that the information has been destroyed; or
- simply return the mail to the sender (rather than destroying it).

Arguably the former patient would still "reasonably expect" (APP 6.2(a)) the practice to do one or more these things, notwithstanding that they have withdrawn their consent. Item 1 of section 16A also allows use, collection or disclosure without consent where:

> *(a) it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure; and*
> *(b) the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.*

Clearly, it would be unreasonable or impracticable to obtain the former patient's consent if the practice does not have their current details. But, if practice does have their details, would they be in breach of Proposal 11.3 if they used these details to notify them of the new information?

Proposal 12 – Fair and reasonable personal information handling

Proposal 12.1 recommends that the government amend the Privacy Act to:

> *introduce a requirement that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances.*

This would be an objective test. It would apply to not apply to collections, use or disclosures under APP 3.4 or APP 6.2(b) to (e) (Proposal 12.3). It would apply where a practice is relying on:

- express patient consent (APP 3.3 and APP 6.1); or
- what the patient would reasonably expect (APP 6.2(a)).

This means that the new test:

- will not apply if a doctor is defending a "claim" (APP 6.2(c) and Item 4) or relying on a statutory authorisation to disclose information; but
- will apply if a doctor is defending themselves a complaint or responding to a "Please explain" letter.

The Report proposes that the legislation contain a list of factors that may be taken into account in determining whether a collection, use or disclosure is fair and reasonable in the circumstances (Proposal 12.2). These factors include:

> *(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances*
>
> *(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency*
>
> *(d) the risk of unjustified adverse impact or harm*
>
> *(e) whether the impact on privacy is proportionate to the benefit*
>
> *(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.*

The Review states (on page 117) that:

> *Legislated factors relevant to assessing fairness and reasonableness would provide APP entities with clarity in considering whether their acts and practices satisfy the test. Including the factors in legislation would provide binding guidance to the IC and the courts when applying the test in different factual circumstances. The legislative factors should be non-exhaustive and not operate as standalone tests, as different circumstances will require a balancing of different considerations to ensure a contextual assessment of fairness.*

In our view, a list of non-exhaustive factors that need to be balanced against each other will not provide APP entities with clarity. Practices will need considerable guidance as to what is or is not "fair and reasonable", particularly if the disclosure is not in the individual's "best interests". For example, is it "fair and reasonable" for a doctor to volunteer patient information to respond to a complaint to the Medical Board? What if the patient is a child?

This uncertainty is compounded by Proposals 16.4 and 17.1.

- Proposal 16.4 requires *entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances*

  It is unclear whether this proposal is simply a restatement of Proposal 12.2(f) or whether, unlike proposal 12.2(f), this is also intended to apply to collections, use or disclosures under APP 3.4 or APP 6.2(b) to (e).

- Proposal 17.1 states that (page 159):

  While the 'fair and reasonable test' would be assessed objectively, where an entity is aware that it is likely to be handling information of people experiencing vulnerability, or is engaging in activities which could have a significant effect on people experiencing certain vulnerabilities, those circumstances will be relevant to whether the entity's information handling objectively satisfies the fair and reasonable test. Any information the APP entity has, or ought to have, about the likely vulnerabilities of their users would be relevant in determining whether a collection, use or disclosure is fair and reasonable in the circumstances.

Doctors provide health services to children and other vulnerable persons. They need certainty about their ability to use and disclose health information for related purposes. These include purposes (such as responding to patient complaints or following up debts) that may not be in the best interests of the child or vulnerable person.

We support the comments on page 118 of the Review:

> *individuals do not have an absolute interest in privacy and … in many cases, personal information handling activities provide benefits to society.*
>
> *For example, the processing of personal information may be an important part of securing societal interests such as the health and safety of other individuals, or for socially beneficial healthcare research. Similarly, APP entities may be required to process personal information as part of … processing payment for products and services that they have offered to consumers. It is envisaged that a reasonable person would consider it fair and appropriate for these legitimate and important practices to be undertaken.*
>
> *OAIC guidance could list practices that will ordinarily meet the fair and reasonable personal information handling test, including legitimate business activities such as fraud detection and prevention…*

Page 119 of the Review also acknowledges that there are circumstances where handling of information may be detrimental to the individual (but this detriment is justified). However, the examples provided relate to the ATO or law enforcement. These entities will usually have the benefit of the "required or authorised by law" exemption. Proposal 12.2 is not intended to apply

in circumstances (such as subpoenas or notices to produce) where an APP entity is authorised or required by law to disclose personal information (Proposal 12.3). However, it is less clear whether Proposal 16.4 (which relates to children) would apply in this case.

The Review suggests that the Explanatory Memorandum (rather than the legislation itself) could contain further information on relevant considerations for considering what is "proportionate":

- *whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent*
- *whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and*
- *any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.*

No rationale is given for including some factors in the Act and other information in the Explanatory Memorandum or guidance documents.

Proposal 13.1 – Require APP entities to conduct privacy impact assessments for "all activities with high privacy risks"

Proposal 13.1 of the Report is that all APP entities conduct a privacy impact assessment (PIA) for "all activities with high privacy risks". Currently this is mandatory for government agencies and optional for other APP entities. It is unclear whether a failure to prepare a PIA will constitute an interference with privacy. OAIC will also be empowered to request a copy of the PIA.

The Report proposes that:

- *The Privacy Act define a "high privacy risk activity" as one which is "likely to have a significant impact on the privacy of individuals." Specific high-risk practices could also be set out in the Act.*
- *OAIC develop guidance which articulates factors that that may indicate a high privacy risk, and provides examples of activities that will generally require a privacy impact assessment to be completed.*

The Report provides (on page 124) an indicative list of high privacy risk activities that could be listed in the Act or OAIC guidance. This list includes:

- *the collection, use or disclosure of sensitive information on a large scale*
- *the collection, use or disclosure of children's personal information on a large scale.*

The term "large scale" is not defined.

The Report goes onto note (on page 159) that:

> *A list of factors indicate when a project may be high risk, including: 'handling personal information of individuals with particular needs.' Given the breadth of vulnerability factors that may cause a person to be more susceptible to harm, it is proposed that an entity conduct a PIA before commencing an activity where the entity is aware, or ought to be aware, that an individual (or group of individuals) is experiencing vulnerability and the activity might have a significant effect on that individual (or cohort).*

The Report proposes (Proposal 17.1) that OAIC guidance include a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information. This list is likely to include older persons, persons with disability and persons with mental health and physical health conditions. Doctors treat people in these groups every day.

The AMA seeks assurance that Proposal 13.1 (as supplemented by Proposal 17.1) is not intended to capture the ordinary collection and disclosure of personal information that occurs as part of providing medical services to patients. It is not reasonable to expect every doctor who wants to start a new private practice, or a new GP clinic opening in rural area, to conduct a PIA. PIAs are generally conducted for government agencies by in-house privacy teams or specialist privacy lawyers or consultants. The changes to the Privacy Act are likely to further increase the cost of (and demand) for PIAs. GP clinics (particularly in rural areas) and small specialist practices simply do not have the capacities of government agencies to pay for these types of assessments. The burden on the health sector will be even greater if this change is intended to apply to existing practices.

By contrast we appreciate that the collection and disclosure of health data (including by doctors) may be high privacy risk. Examples include:

- Health apps
- Private health insurers (as illustrated by the Medibank data breach)
- My Health Record
- Medical software providers
- Large businesses (including some private health insurers and private hospitals) that own or operate health businesses and share data or store data centrally
- Online businesses that only offer online telehealth/ script services (particularly where the service is foreign owned or stores data outside Australia)
- Multinationals that are increasingly expanding into the healthcare space.[2]

Accordingly, the AMA supports and welcomes provision of explanations and examples of when this new requirement will apply, particularly in the health sector.

[2] See for example: One Medical joins Amazon to make it easier for people to get and stay healthier https://www.aboutamazon.com/news/company-news/one-medical-joins-amazon-to-make-it-easier-for-people-to-get-and-stay-healthier or Google Health Privacy Matters https://health.google/privacy/

Proposal 13.4 – Amend APP 3.6 to require third parties to take reasonable steps to satisfy themselves that the information was originally collected from the individual in accordance with APP 3

This proposal has been amended (since the Discussion Paper) to include provision for the OAIC guidelines to provide examples of reasonable steps that could be taken. The AMA would appreciate this guidance, particularly in the medical sector. For example, the Report states (on page 130) that:

> *In some circumstances, no steps would be reasonable, for example, where a GP has provided a referral to a specialist it would generally not be necessary for the specialist to take steps to satisfy themselves that the information was originally collected from the individual in accordance with APP 3.*

Similarly, a GP should not be required to verify that personal information contained in report from a non-GP specialist, allied health provider or hospital was originally collected from the individual. As discussed above, in many cases, the report will contain information that was inferred by the health provider. The Report treats this as a "collection" (Proposal 4.3).

There may also be instances where a GP receives information from a third party (such as a pathologist or an instant script provider) but has no direct dealings with that third party. Again, it is reasonable for the GP to assume that the original collection was fair and reasonable and otherwise in accordance with APP 3.

It also should be clarified how Proposal 13.4 is intended to apply in situations where the patient cannot personally consent to collection. For example:

- A doctor may receive pathology results or a referral in relation to a baby. The doctor should not be required to check that the pathologist or referring doctor collected the personal information in accordance with APP 3.
- A medical journal may publish a study about treatment of patients with dementia. The contract with the author would include standard provisions about privacy and ethics but the journal should not be required to undertake any further due diligence.

We assume also that this amendment is not intended to apply retrospectively (i.e., to personal information already in the hands of the third party). This should be clarified.

Proposal 14 – New exception for research

Our submission to the Discussion Paper raised multiple concerns about the impact of the proposed changes for medical research. We therefore welcome proposals to:

14.1 Introduce a legislative provision that permits broad consent for the purposes of research.

14.2 Consult further on broadening the scope of research permitted without consent under the Act for both agencies and organisations.

14.3 Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.

The AMA looks forward to being involved in this consultation. In particular, while we support medical research, we are mindful that not all "research" is in the public interest, particularly where carried out by for profit organisations. Page 137 of the Report emphasises that:

> *If the scope of the exceptions is expanded, the existing safeguards would continue to apply. Agencies and organisations would need to obtain HREC approval for the proposed handling of personal and sensitive information without consent, for which they would need to demonstrate the impracticability of obtaining consent and that the activity cannot proceed on the basis of de-identified information.*

Proposal 15.1 – New obligations to determine and record primary and secondary purposes

Proposal 15.1 introduces an express requirement to record:

- the primary purpose for collection, use and disclosure at the time of collection; and
- any secondary purpose, prior to undertaking secondary use or disclosure.

This is in addition to the requirement to:

- have a privacy policy;
- issue an APP 5 notice;
- only collect information where permitted by APP 3; and
- only use or disclose information where permitted by APP 6.

It appears (from the explanation given on 143) that the primary purpose of this additional record keeping is to ensure that APP entities turn their mind to relevant APPs when collecting, using and disclosing personal information. It may also be to improve the ability of the individual or third parties (such as OAIC) to audit compliance.

> *The identified purposes for collection, use and disclosure of personal information could also be scrutinised for whether they are reasonably necessary for the entity's activities or functions. Where an entity proposes to handle the personal information of a child, identifying and recording relevant purposes would enable scrutiny of whether the purpose is in the child's best interests.*

Benefits need to be weighed against the administrative costs, particularly for small businesses such as GP and non-GP specialist practices, who often have less than 1 FTE providing

administrative support. It is not realistic to make a separate record for the purposes of the Privacy Act every time a doctor sees the patient, receives test results, makes a diagnosis, makes a referral, receives a report, issues a bill or interacts with Medicare. Page 143 of the Report notes that the steps taken to comply with Proposal 15.1:

> *should be reasonable and proportionate to privacy risks. In most cases, an APP entity would only need to record the types of purposes for which the entity generally handles types of personal information, rather than keep individual records for each piece of information. In cases where collection and use are self-evident from how the information is held (e.g. a customer contact list) no further record would be required unless the information were to be used for a secondary purpose. The requirement to record secondary purposes would apply at or before the point of use or disclosure, rather than at the point of collection when possible future secondary purposes may be unknown.*

Whether or not something is a secondary purpose or part of the primary purpose can be a difficult question in practice. For example, is issuing an invoice (or following up non-payment) part of the primary purpose if it was not expressly referred to in the original collection notice? What about responding to a patient complaint or a query from Medicare? Either way, it would appear that the doctor needs to be able to point to some "record" (made either at the point of collection or the point of secondary use or disclosure) that they use. Medicare will usually query specific item number(s) across multiple patients. Does the doctor need to consider each patient separately and record a separate note in their file?

As written Proposal 15.1 would also appear to require a doctor to make a separate record for the purpose of the Privacy Act before responding to a subpoena or notice to produce. The rationale for this is unclear given the subpoena and response will both be on the file. Will the failure to create a record about the secondary purpose constitute a breach of the APPs (and hence an "interference with the privacy of an individual") even though the doctor is legally required to disclose, this is an exception to APP 6 and there is no requirement for the doctor to consider whether disclosure is fair and reasonable? If so, the AMA considers this approach not just administratively burdensome for doctors, but also potentially resulting in avoidable complaints or investigations.

Proposal 15.2 – New obligation to designate a senior employee responsible for privacy

Proposal 15.2 requires all APP entities to appoint or designate a senior employee responsible for privacy within the entity. This Proposal is clearly directed at larger organisations and fails to consider the impact on smaller organisations, particularly medical practices. GP practices, smaller specialist practices, and rural practices are already experiencing workforce shortages and increasing costs associated with running a practice. For many practices there will be no senior staff beside the doctors, such that a doctor will need to be formally designated as responsible for privacy. If this doctor is a director then they are already legally responsible for the privacy of the entity but a failure to appoint or designate them as having this responsibility would be a breach of the APPs and technically an "interference with the privacy of an individual".

The AMA calls for this proposal to only apply to larger organisations (e.g., 20 or more employees) and/ or for medical practices to be excluded.

Proposal 16.2 – Capacity for children under 18 to consent

The AMA welcomes the substantial revision to these proposals. In particular, the AMA welcomes the Report's recognition that:

- there may be circumstances where it would be harmful to the child or contrary to their interests to require parental or guardian consent to collection, use and disclosure of their personal information; and
- a doctor may determine that a child under 15 has the capacity to consent to collection, use and disclosure of their personal information for the purposes of receiving healthcare.

Proposal 16.4 – Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances

The AMA supports this proposal subject to:

- the new research exception
- clarification that this requirement does not trump other rights (such as the right for a doctor to have their invoice paid or to defend themselves against legal action or patient complaints).

Proposal 18.1 – Replacement of the right to access with a right to "access and explanation"

Patients have an existing right under APP 12 to access their personal information. Proposal 18.1 gives patient additional rights to require practices to:

> *(b) identify the source of the personal information [they have] collected indirectly*
>
> *© provide an explanation or summary of what [they have] done with the personal information [they have collected].*

The format for the response "*should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information"*. The practice may:

> *(d) consult with the individual about the format for responding to a request, and the format*
> *(e) charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual.*

The AMA has significant concerns as to how this would be implemented in the healthcare space. Currently doctors can refuse to give a patient access to health information if they have reasonable grounds for believing it would pose a serious threat to the life, health or safety of the patient or

another person, or to public health or safety. The AMA submits that this exception should be maintained. The discussion (on page 180) acknowledges that:

> *[The UK has] some specific sub-exceptions, **for example 'serious harm' in the case of health data for the right of access**. General exceptions with specific sub-exceptions relevant to specific rights where appropriate could be adopted in the Act, subject to further consultation on the precise content of each general exception.*

There is also a lack of clarity about what a doctor is meant to provide to a patient in relation to a request. Pages 170-1 of the Report states that:

> *The objective [is] to inform the individual as far as is reasonable about what is being done with their information. It should include sufficient detail to put the individual in a position to exercise other rights should they choose, or to furnish a complaint to the OAIC should they have concerns about the APP entity's compliance with the Act.*
>
> *An explanation should inform the individual about what personal information is held and what the APP entity does with it rather than necessarily the substance of the information. **For example, where the personal information may require expertise to understand (e.g. medical information) then it may not be reasonable to explain the information as that should be done in a consultation with the individual's doctor.** It may also not always be reasonable to provide an explanation of all technical data, because it may be unlikely to reduce operational costs while proving unhelpful by risking a misunderstanding between the individual and the entity. Rather an explanation needs to suit its context. An APP entity should be required to explain with sufficient specificity in the circumstances what the information is and detail how it came to hold the information and what it is doing with it.*

While we appreciate acknowledgement of the AMA's submission, it is still unclear how much detail is required. Can the doctor simply say they have used information from the patient, pathologists, diagnostic imaging providers and other specialists to diagnose, treat and invoice the patient and submit claims to Medicare or their private health insurer or is the expectation that the doctor will list every item and how it was used and disclosed? Or is the focus on less routine disclosures (such as subpoenas, Medicare audits and PSR)? As noted above, a Medicare audit will usually be several items across multiple patients so there is some administrative cost in determining whether a specific patient's data has ever been requested.

To give an extreme example, is the intention that a doctor could be required to produce (for a nominal fee) a PowerPoint presentation explaining the role of each participant in the health care system (GPs, non-GP specialists, pathologists, diagnostic imaging, public and private hospitals, private health insurers, Medicare, Ahpra, the Medical Board, Professional Services Review and in some cases courts) and how health information routinely moves between them?

Proposal 18.3 – Right of erasure

We continue to have concerns about any application of the proposed right of erasure will apply to health records, including records held for former patients or by retired health practitioners.

While patients have a statutory right to control (or erase) their My Health Record, this does not extend to the health practitioner's own records. Best practice is for medical records to be held for 7 years or, where the patient is under 18, until they are 25. In some States this is also a legislative requirement.

Proposal 18.3(c) now provides that:

> *In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.*

The AMA argues that in the healthcare space, certain information should remain available for purposes broader than just law enforcement. Those purposes should include Medicare compliance, Professional Services Reviews, Ahpra and Medical Board of Australia complaints handling, doctors' indemnity insurance, and similar.

Proposal 18.6 refers to three categories of general exemptions that would apply to access, correction and erasure requests. These categories are:

> *(a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities.*
>
> *(b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual.*
>
> *(c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request.*

As noted above, exceptions should also be allowed for research and healthcare and medical care situations. The Report acknowledges (on pages 180 and 181) that:

> *The majority of [UK exceptions to the GDPR], such as freedom of expression, **research, and health data**, are expressed to apply to all rights. Within these exceptions, there are some specific sub-exceptions, **for example 'serious harm' in the case of health data for the right of access**. General exceptions with specific sub-exceptions relevant to specific rights where appropriate could be adopted in the Act, subject to further consultation on the precise content of each general exception.*
>
> *The Act currently recognises exceptions to certain requirements in the Act for collection, use and disclosure of information in some **health care situations and human-based research**. Having regard to the public interest in **effective and informed health care and research, consideration should be given to applying health care and research exceptions to the rights of the individual**.*

There also needs to be greater clarity about how these exceptions apply in relation to new proposal 18.3(b). It requires practices that have collected information from a third party (or provided information to a third party) to:

> *inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.*

Is this obligation only intended to apply where the APP entity is required to destroy the records (i.e., there is no relevant exception) or is it a free standing obligation? For example, if a person asked their GP to delete their records (and the GP was entitled to say no), would the GP still be required to inform other specialists (such as pathology and imaging providers) of the request?

We note also that it is common for a person's medical record to include information about family members, particularly where the condition is genetic. This is an existing permitted general health situation (item 1A of section 16B). This exception should continue to override any obligation to erase and there should not be an obligation to inform these family members of an erasure request.

Proposal 18.4 – Extend right to correction to online publications

In our previous submission, the AMA noted that it would be impractical (and inadvisable) to correct information in published journals, including such information as author names or qualifications. Proposal 18.4 extends the right to correct to online publications (such as websites) that are controlled by an APP entity.

However, it acknowledges (on page 177) that:

> *[There] will be times where the public interest in freedom of expression or academic research does not favour a correction of an online publication. The entity would instead assess the request in light of the general public interest exceptions discussed [in Proposal 18.6]."*

Page 180 notes that:

> *The Discussion Paper considered that an exception to the right to erasure could be modelled on the public interest test in the FOI Act with factors that could guide decisions about what was in the public interest:*
> - *promotion of the objects of the Act*
> - *informing the public, or enabling debate on a matter of public importance*
> - *constituting an unreasonable limitation on the expression of a legitimate view or opinion, or*
> - ***inhibiting the handling of personal information for archival, research or statistical purposes, journalistic purposes; or for academic, artistic or literary expression in the public interest.***

While most valuable for the right to erasure, an exception for freedom of expression based on the FOI Act test could be recognised as part of a public interest exception which could potentially apply to other rights, if relevant."

The AMA looks forward to seeing further detail about this proposed exemption.

Proposals 18.8 – 18.10 – Additional obligations on APP entities in responding to requests

Proposals 18.8 to 18.10 contain new obligations on APP entities (including medical practices) to:

18.8 provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.

18.10 acknowledge receipt of a request to exercise a right of the Individual within a reasonable time and provide a timeframe for responding.

Also, under 18.9 it is proposed that:

18.9 take reasonable steps to respond to an exercise of a right of the individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.

What constitutes "reasonable assistance" is undefined. Page 184 states that:

The OAIC recommended a requirement modelled on existing FOI requirements to provide 'reasonable assistance' to individuals to reframe their request and provide them with a reasonable opportunity to revise a request, before the request is refused. An obligation on APP entities to provide reasonable assistance to individuals to exercise their rights would address the imbalance in understanding between the APP entity and the individual, whilst facilitating the relationship between the parties. For example, an individual could object to a particular use which arises from the way in which the individual engages with a service, and rather than ceasing the relationship, the APP entity could erase one set of information but assist the individual to re-engage with the service on a different, mutually agreed basis. Reasonable assistance would enable the individual to exercise their rights, without a technical or legalistic approach to the wording of a request, which may not be in the interests of either party.

FOI requests are, by definition, made to government agencies that often have whole teams dedicated to responding to FOI requests. A medical practice may be a single doctor and a part-time administrator. They do not have the resources to assist individuals to "reframe" access requests and it is not realistic for a patient to ask for erasure of some of their medical records to opt out of some secondary purposes (such as billing or Medicare audits). Other types of requests (e.g., not to report back to a GP) are already accommodated.

The AMA strongly recommends that these kinds of obligations be reconsidered for small entities (e.g., under 20 staff). At minimum OAIC should produce a form of wording that in its view satisfies Proposal 18.9 (notification of right to appeal).

Proposal 20.1 – Direct marketing, targeting and trading

The AMA has concerns around how what is proposed under Proposal 20.1 may inadvertently impact medical professionals. The proposal is to introduce definitions of "direct marketing", "targeting" and "trading". The latter two terms are defined as:

> *Targeting –the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).*
>
> *Trading –the disclosure of personal information for a benefit, service or advantage.*

Ordinary medical services may fall within both these definitions. Doctors collect patient information to provide health services that are tailored to them. In some cases, they may withhold information from them because it may damage their mental health. They may also withhold treatment options from them which are unsuitable for them. Doctors also disclose health information to other organisations (particularly Medicare and private health insurers) in order to receive payments. However, usually this will occur with express patient consent.

We assume that Proposal 20.7 (prohibition on trading in personal information of a child) is not intended to prevent doctors from submitting claims to Medicare or private health insurers in relation to children. Similarly, we assume that Proposal 20.8 (prohibition on targeting based on sensitive information) is not intended to prevent doctors from taking into account race when treating patients. For example, First Nations Australians were provided with earlier access to Covid vaccines because they are a higher risk health group.

Proposal 20.4 – Require an individual's consent to trade their personal information

Proposal 20.4 of the Report is that a requirement be introduced to obtain an individual's consent to "trade" their personal information. The AMA supports this proposal. Online platforms, such as instant scrip providers and clinical information systems are increasingly trading patients' personal health information for profit. The AMA does not support sharing health information with private health funds outside the existing statutory schemes. It is the AMA position that patients' medical information must be protected to maintain the clinical independence of their healthcare pathway.

Proposal 21 - Security, Destruction and Retention of Personal Information

Proposal 21.1 to 21.3 – Security of personal information

The Report acknowledges that current APP 11.1 requires APP entities who hold personal information to take such steps that are reasonable in the circumstances to protect that personal information from misuse, without explaining what is considered to be 'reasonable steps'. This approach was deliberate, so as to give APP entities flexibility to determine what steps may be reasonable for them in their circumstances. The Report then proposes (Proposal 21.1) that the government:

> *21.1 Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures.*

The AMA agrees that this change would not (and should not) provide greater specificity as to what reasonable steps APP entities should be taking. In the context of medical practices, particularly small GP and non-GP specialist practices, reasonable steps may be different to the steps that would need to be taken by private health insurers who hold vast amounts of patient data. Reasonable steps should be commensurate with the risk of organisations being exposed to security breaches. Larger 'honey pots' are more attractive targets for hackers.

The concept of a "reasonable organisational measure" should also be commensurate with the size of the organisation. In particular, in line with our comments on Proposal 15.2 above, any requirement for organisations to designate a senior employee responsible for privacy should only apply to larger organisations (e.g., 20 or more employees) and/ or medical practices should be excluded.

In terms of reasonable technical measures, the AMA is supportive of strong requirements for data governance frameworks that support the quality, security and privacy of the patient data. In the AMA's 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.[3]

The Report proposes (Proposal 21.1) that the government amend APP 11 to insert a list of outcomes-based factors that APP entities should consider. All entities would have to ensure that their practices would meet these outcomes. This may require upgrades to an entity's information security capacities. The Report goes onto propose that the government:

> *consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.*

The AMA is supportive of the approach to align the amendments to the Privacy Act with the 2023-2030 Australian Cyber Security Strategy. However, we anticipate that GPs and non-GP specialists in private practice will need financial and other assistance to meet these requirements.

[3] https://www.ama.com.au/articles/ama-position-statement-data-governance-and-patient-privacy

Proposals 21.4 and 21.5

Proposal 21.4 is that the government:

> *Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information*.

The AMA understands that this Proposal is linked to Proposal 4.5 (which proposes that de-identification not be a one-off process) and Proposal 4.6 (which proposes that APP 11.1 be extended to de-identified information.)

As outlined above, the AMA is supportive of Proposal 4.6, and consequently Proposal 21.4, because it requires APP entities that hold information:

- to continuously consider whether that information is appropriately secured;

At the same time, it does not require them to retrospectively comply with provisions (particularly APP 3 and APP 5) that apply to identifiable information.

We also support Proposal 21.5 and the comments on page 226 of the Report:

> *although principles-based regulation is desirable, APP entities require more specific guidance to understand the extent of their obligations as well as modern, relevant advice as to what steps may be reasonable in the context of their operations (e.g. healthcare and research). Enhanced guidance could be applied by APP entities according to the specific industry, method of destruction and/or the type or sensitivity of the information.*
>
> *… the most effective way to address this issue would be through OAIC guidance. The guidance in relation to APP 11.2 could be enhanced to cover both destruction and retention matters, as well as de-identification matters.*
>
> *21.5 The OAIC Guidelines in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.*

Proposals 21.7 and 21.8 – Retention

The Report acknowledges (on page 228) that:

> *providing APP entities with the flexibility to set their own retention periods, consistent with retention requirements under APP 11.2 would also enable them to tailor retention periods according to the type of data. This would assist industries where the management of personal information can be more complex, such as* ***in the healthcare sector where it can be challenging for smaller providers who hold numerous sets of health data where those records become no longer required at different times***.

The Report goes on to propose (Proposal 21.7) that the government:

> *Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need.*

It is the AMA's view that this approach would be beneficial for smaller medical practices, provided that the drafters considers both legislative and non-legislative for retaining information. As noted above, retention periods for medical records are legislated in only some states. However, in all cases, best practice is for medical records to be held for 7 years or, where the patient is under 18, until they are 25.

We also note that, while health data may no longer be required to be kept for the individual patient (particularly where the patient is deceased), it may also be useful and beneficial to maintain it for longitudinal studies for example, or for research purposes in General Practice or for electronic decision support systems (eCDS). It is also common for patient health information to be held on records relating to their family members (particularly where there is a genetic condition).

Proposal 21.8 recommends that the government

> *Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods*.

While the AMA is supportive of transparent and accountable health data handling by entities,[4] we believe this requirement may be impractical particularly for smaller entities and inconsistent with the overall objective of ensuring that privacy and other policies are user-friendly. The Attorney-General's own records disposal policy is 170 pages.[5] While not all of these documents will contain personal information, APP entities will need to consider a wide range of documents. They will also need to consider potential changes to the employee records exemption. While the Report claims that Proposal 21.8 would be in line with Article 13 of the GDPR, in practice European organisations do not specify personal information retention periods in their Privacy Policies. For example, the Privacy Policy of the British Medical Association states that:

> *We keep personal data for as long as necessary to ensure we can deliver our services in line with our retention policy. This policy reflects legal requirements, our regulatory and compliance functions, and other applicable considerations to determine the appropriate*

[4] Australian Medical Association 2023. AMA Position Statement on Data Governance and Patient Privacy 2022. https://www.ama.com.au/articles/ama-position-statement-data-governance-and-patient-privacy
[5] Attorney General's Department 2022. Records Disposal Authority Attorney-General's Department https://www.naa.gov.au/sites/default/files/2019-12/agency-ra-2002-04572652.pdf

retention period. We do not retain personal data in any identifiable form for longer than is necessary.

We note also that, while it may be feasible for larger entities (such as Attorney-General's) to employ people to sentence records on a daily, monthly, quarterly or annual basis, this is not feasible for smaller entities, particularly GPs and small specialist practices. As noted earlier, best practice is for a doctor to retain a complete record for all current patients. If the doctor closes the practice, the doctor (or their estate) may be required to keep records for up to 25 years (depending on the age of the patient). While best practice would be to regularly destroy records that have expired, few retirees have these kinds of resources.

Proposal 23.5 – Require APP entities to specify in APP 5 notices the types of personal information that may be disclosed to recipients located overseas.

Entities will need some time to update their APP 5 notices to ensure that they specify the types of personal information that may be disclosed to overseas recipients.

These updates will also be impacted by proposal 23.6, which clarifies that hosting by secure Cloud Service Providers located overseas does not constitute a "disclosure". We also support the proposal (also part of proposal 23.6) that further consideration should be given to whether online publications of personal information (e.g. on a website) should be excluded from the requirements of APP 8 where it is in the public interest.

25. Enforcement

The Report rightly identifies the issues with the current framework, and the limited powers of the Information Commissioner.

Under 25.1, the Report then goes on to propose to:

- Create tiers of civil penalty provisions to allow for better targeted regulatory responses:
(a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.
(b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.

The AMA understands that the intention of this proposal is to introduce a penalty high enough to ensure deterrence, however we argue that penalty in itself will not achieve the desired outcome, but may result in financial unsustainability of smaller medical practices.

It is known that health data is more valuable than other personal data,[6] and that actors with malicious intent tend to target health more. Health service providers have continuously been in

[6] See for example this article: Hackers breaches value health data 2022. https://www.linkedin.com/pulse/hackers-breaches-value-health-data-2022-e-book-update-mesk%C3%B3-md-phd/?trk=pulse-article_more-articles_related-content-card

the top 5 sectors to notify data breaches in Australia, commonly number one. Major source of data breaches in the health space are malicious or criminal attacks, followed by cyber incidents.[7]

The Report then provides an explanation what would be considered an *interference with privacy without a 'serious' element:*

> *Proposal 25.2 – Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include:*
> *(a) those involving 'sensitive information' or other information of a sensitive nature*
> *(b) those adversely affecting large groups of individuals*
> *(c) those impacting people experiencing vulnerability*

Medical practices by definition handle sensitive information about people experiencing vulnerability. At the same time, they are more exposed to malicious attacks and cyber incidents. This proposal will mean that any breach by a medical practice would be treated as a "serious" interference with privacy. Accordingly, we call for:

- greater clarity about what types of breaches will be considered an "administrative breach" of the Act or the APPs. For example, would a failure by a GP to conduct a privacy impact assessment or formally designate themselves as the privacy officer be an administrative breach?

- retention of some element of failure to meet community expectations in the concept of a 'serious' interference so that small practices are not subjected to a 'first strike' offence that does not apply to other sectors of the community.

Proposal 25.5 – Ability of OAIC to direct APP entities to perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/ those individuals

In our submission to the Discussion Paper, the AMA argued against the proposal to require APP entities to identify, mitigate and redress actual or reasonably foreseeable loss. The new formulation in the Report fails to address the AMA's concern. While it proposes that the OAIC publish guidelines on "how entities could achieve this", it continues to put the onus on the organisation (which may be a sole practitioner) to identify any loss or damage that could be suffered because of a breach. This is something that they would need to outsource. Even then they might 'get it wrong', by failing to:

- Identify a reasonably foreseeable loss or damage; and
- Mitigate a reasonably foreseeable loss or damage.

[7] OAIC 2022. Notifiable data breaches report January to June 2022. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2022

We continue to submit it should be the OAIC to identity the reasonable loss and the mitigation steps required, so that doctors know what they are being directed to do. Otherwise, doctors are exposed to 'double jeopardy' for the same original breach.

In our previous submission, we also noted that the standard "reasonably foreseeable loss or damage" is a much lower standard than the standard under the Notifiable Data Breach scheme both in probability (likely vs. reasonably foreseeable) and quantum (serious harm vs. any loss or damage).

Proposal 25.7 – Industry funding model

The Report proposes under 25.7 that

> *Further work should be done to investigate the effectiveness of an industry funding model for the OAIC*.

We prefer this proposal to Proposal 24.7 of the Discussion Paper, which called for an introduction of an industry funding model similar to ASIC, that would incorporate a statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment. The AMA was not supportive of this proposal. We were concerned that this formulation may result in an imposition of a 'privacy tax' on medical practitioners/practices.

However, further details are required as to how "industry" is defined and what kind of contribution would be expected from each entity, particularly entities with under 20 staff.

Proposal 26.1 – Direct right of action

The AMA did not support the Discussion Paper's proposal to create a direct right of action. We said that, if a right of direct action is introduced, there should be a gateway of the type proposed in the Discussion Paper and that it should be limited to serious and repeated breaches of privacy.

The Report recommends (Proposal 26.1) that the government:

> *Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy.*

The proposed model has following design elements:

(a) *The action would be available to any individual or group of individuals who have suffered loss or damage as a result of privacy interference by an APP entity.* ***This would include claims by representative groups on behalf of members affected by breaches of the Act.***
(b) ***Loss or damage would need to be established within the existing meaning of the Act. [This may include] injury to the person's feelings or humiliation****.*
(c) *The action would be heard by the Federal Court or the Federal Court and Family Court of Australia (FCFCOA).*

(d) *The claimant would first need to make a complaint to the OAIC and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme.*

(e) ***Where the Information Commissioner or an EDR is satisfied there is no reasonable likelihood that the complaint will be resolved by conciliation or the IC decides a complaint is unsuitable for conciliation, the complainant would have the option to pursue the matter further in court**.*

(f) In cases where the Information Commissioner has decided that a complaint is unsuitable for conciliation on the basis that the complaint does not involve an interference with privacy or is frivolous or vexatious, the complainant should be required to seek leave of the court to bring an application in the court.

(g) *The OAIC would have the ability to appear as amicus curiae or to intervene in proceedings instituted under the Privacy Act, with leave of the court.*

(h) *Remedies available under this right would be any order the court sees fit, including any amount of damages*.

Highlighted in bold above are the amendments in comparison to what was proposed under the Discussion Paper.

The AMA continues not to support this proposal. The formulation above is not limited to serious interferences with privacy and allows actions (including class actions) to be brought on the basis of hurt feelings. At minimum, administrative breaches (such as a failure to nominate a privacy officer, a failure to respond to an erasure request within a statutory time frame or failure to provide a person with a compliant statement about their rights to sue) should not found a cause of action.

Throughout our submission we have also given examples of scenarios that are not 'black and white' and will become more complex to navigate if the APPs are amended as proposed. In these situations, the direct right of action provides another forum for disgruntled patients to litigate (or to threaten to litigate). For example, a patient who is not satisfied with the outcome of a medical procedure may already sue for negligence and complain to the Medical Board. If the doctor volunteers patient information to defend themselves and it is not clear cut that the doctor will have the benefit of an exception to the APPs, the patient may expand their legal claim to include damages for interference with privacy. Dealing with the additional claim increases insurance premiums, which are ultimately a cost to the health system.

Proposal 27.1 – Statutory tort for serious invasion of privacy

As stated in our previous submission to the Discussion Paper, the AMA does not support the establishment of statutory tort, particularly if it will allow yet another forum to litigate the same issues.

The new proposal in the Report maintains the same approach as the Discussion Paper, suggesting further consultation with the states and territories to ensure that the tort is formulated in a consistent way across jurisdictions:

27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.

Proposals 28.1, 28.2 and 28.3 – Notifiable data breaches scheme

The Report recommends (Proposal 28.1) that further work be undertaken to:

better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

We support this proposal. As highlighted in our previous submission, doctors have different reporting obligations for the same data depending on the jurisdiction and whether it is held in a My Health Record or the doctor's own records.

Proposal 28.2 recommends that the government:

- *Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.*
- *Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.*

We support both these amendments. While "eligible data breaches" are limited to those breaches that are likely to cause serious harm, the Optus and Medibank Private hacks have illustrated that they do occur, and the public expect to be informed as soon as practicable so that they can be aware of the threat and take steps to protect themselves.

However, we have some concerns about the last paragraph of Proposal 28.2. It recommends that APP entities be required:

- *to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.*

It is not clear what this means in practice, particularly for small entities. The preceding paragraph states that:

- *To further assist an entity to act quickly in the event of a data breach, entities should have a data breach response plan. Although entities may already be required to do this under APP 1 and APP 11, an express provision to this effect in*

> *the NDB provisions would provide certainty and ensure that entities proactively plan for how they would respond to a breach, including how they would notify individuals.*

Again, this is something which is more appropriate to larger entities (e.g., more than 20 employees). We also recommend that OAIC provide templates for particular industry sectors that meet this requirement. For the health sector this could be an updated version of the guidance at https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/health-service-providers/data-breach-action-plan-for-health-service-providers

We also recommend that it be clarified that a failure to maintain a data breach plan is an administrative breach.

Proposal 28.3 recommends that the government:

> *Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates. However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information.*

We support this amendment. However, again, we have concerns about the practical implications of the final part of this proposal:

> *Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach.*

It appears from the text preceding this paragraph that this is referring to large scale breaches involving large, well-resourced entities (such as Optus and Medibank Private). Small businesses (such as private medical practices) simply do not have the resources to do things like:

- paying for a credit monitoring service
- monitoring the dark web to identify if personal information compromised in a data breach is being traded online
- assisting individuals to replace compromised credentials, such as passports and drivers licences
- engaging providers such as IDCARE to provide post-incident support to individuals.

31 March 2023