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

AMA submission to Attorney General's Department – Review of the *Privacy Act 1988*, a response to the Discussion Paper

privacyactreview@ag.gov.au

The AMA welcomes the opportunity to comment on the Discussion Paper. This submission focuses on the proposals and questions posed in the Discussion Paper that are of relevance and may impact AMA members. We also refer to our previous submission.[1]

The AMA has serious concerns with some of the proposals in the Discussion Paper and the impact that they would have on basic medical practice and the feasibility of conducting medical and health research in Australia.

Overview

Many of the Proposals in the Discussion Paper will have a negative impact on health care (for individual patients) and medical research. While the Discussion Paper contains some acknowledgement of the need to preserve existing exceptions for healthcare and medical research, new exceptions will be required to mitigate or avoid these impacts. For example, unless there is an exception for health care:

- **Proposal 2** would require practitioners to notify patients and seek their consent every time they receive pathology results.
- **Proposal 10** would inhibit (and in some cases prohibit) medical research into childhood diseases.
- **Proposal 13** would remove any ability for persons under 16 to seek confidential advice about their sexual or mental health (including through headspace and KidsHelpLine).
- **Proposal 16** would require doctors to repeatedly give patients written notices reminding them that they are trying to influence their behaviour and decisions.

[1] Australian Medical Association 2021 AMA submission to the Attorney General's Department – the Review of the Privacy Act 1988, a response to the Issues Paper

The rationale for many of these Proposals concerns targeted marketing by commercial entities that either operate online platforms or applications or purchase data from entities that do. In the AMA's view, rather than fundamentally changing the Privacy Act, these concerns would be better addressed through separate legislation that applies to prescribed services, organisations or activities.

Proposal 2.5: Require personal information to be anonymous before it is no longer protected by the Act

The AMA does not have any comments on the change from "about" to "that relates to". However, we are concerned about the proposal to add the following words to the end of the definition:

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

Elsewhere in the Review the terms "directly" and "indirectly" are used in the context of the collection of information from either the individual themselves ("directly") or a third party ("indirectly"). In this case, it appears that they are intended to refer to information held by the APP entity or a third party. The Review states (on page 27):

> *"Including the phrase 'directly or indirectly' would make it clearer to APP entities that they should consider other information available when assessing whether information is personal information, including publicly available information where there is a risk that the information could be made public.*
>
> *The new definition could be supported by providing a list of objective factors to help APP entities assess whether an individual is 'reasonably identifiable'. These factors could include the context in which the information is to be held or released, the costs and amount of time required for identification, and available technology. The definition would not capture information where there is only an extremely remote or hypothetical risk of identification.*
>
> *[This] change would also affect how APP entities assess whether information is de-identified or anonymised. Information would need to no longer be related to an identified or reasonably identifiable individual, considering the above definition, for the Act to no longer apply."*

Further information about anonymisation is provided on page 30:

> *"Anonymisation is the process of irreversibly treating data so that no individual can be identified, <u>including by the holders of the data</u>.*

> *Information would be considered 'anonymous' if it were no longer possible to identify someone from the information, considering the definition of 'reasonably identifiable' and the factors outlined in Proposal 2.3.*
>
> *Information could be considered anonymous provided that the risk of re-identification was extremely remote or hypothetical."*

This is a high standard which may require that data be stripped of all information of value to researchers. As noted in the Review (page 128), US researchers have reported that:

> *"between 61 and 87 per cent of individuals in the United States were able to be identified by a combination of ZIP code, birth date and gender."*

Age, sex and postcode are all relevant factors for medical research. The example above uses a person's full birth date. Using only birth year (or even month) makes it much less likely that only one individual would meet the criteria. However, other information (such as the person was treated for a particular cancer) would increase the probability that they could be reidentified.

The Australian Institute of Health and Welfare has submitted that:

> *"Amending the Privacy Act to regulate de-identified information or moving to a higher standard of de-identification could significantly impede medical and other human research that is founded on analysis of de-identified information"*[2]

The AMA shares these concerns. For example, currently GPs provide de-identified data to Primary Health Networks as part of the Practice Improvement Program.[3] Proposal 2.5 would require GPs to consider what other information the recipients have (or may have) and to remove all information that could potentially be used to re-identify the patients. This is notwithstanding that any such re-identification would be unlawful and a breach of the contract. While the AMA supports high de-identification standards whenever health information is involved (see, for example, our submission on the Data Availability and Transparency Bill), there needs to be a balance between privacy and public benefit.[4]

Going forward, the alternative would be for GPs to ensure that they obtain express consent from their patients to participate in the Practice Improvement Program (notwithstanding that only de-identified data are provided). However, we expect that there are existing data that were obtained without express consent. For example, some GPs include a notice about the program in their practice. It will also be impossible for researchers to know whether or not these requirements were met as they do not obtain data directly from GPs.

[2] Australian Institute of Health and Welfare (AIHW) Submission to the Attorney-General's Department in response to Privacy Act Review Issues Paper October 2020
[3] Australian Government Department of Health 2019 PIP QI Incentive guidance
[4] Australian Medical Association 2021 AMA Submission to Data Availability and Transparency Bill

Extension of the definition of "personal information" to individuals who are distinguishable (but not identifiable)

More concerningly, the Review appears to suggest (on pages 27 and 134) that data will be "personal information" if they relate to one individual even if researchers have no way of identifying that individual.

> *"The definition would cover circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named."*
>
> *"Proposal 2.1 to amend the definition of personal information to include a greater range of information and Proposal 2.2 to provide a non-exhaustive list of the types of information capable of constituting personal information – would address concerns that some targeted advertising may fall outside the scope of the Act due to the use of technical identifiers and data to explicitly target an unidentified individual's personal preferences with a high degree of accuracy."*

Treating a set of information about a specific (but unidentifiable) individual as "personal information" has obvious implications for any kind of research that involves unit record data. Researchers routinely use anonymous surveys to collect information from individuals. Each response is allocated a technical identifier and researchers will know (but will rarely publish) the complete set of responses submitted by specific respondents. Similarly, health researchers will use de-identified MBS and PBS data or hospital admission data for individual patients to conduct research. In some cases, researchers will allocate unique technical identifiers that allow them to link unit record data across different time periods for the purposes of longitudinal research (such as long-term outcomes for different types of cancer treatment).

It is also unclear how the inclusion of circumstances "in which an individual is distinguished from others" would apply to photographs of a specific individual that do not include the individual's face or contain any other identifying features (such as a tattoo). Medical journals and medical schools use photographs of medical conditions (e.g. skin cancer) for educational and scientific purposes. If these photos are treated as personal information, then they will be subject to all the proposals in the Review.

Proposal 2.4: Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information

Proposal 8.2: APP 5 notices limited to the following matters under APP 5.2:

- **the identity and contact details of the entity collecting the personal information**
- **the types of personal information collected**

- **the purpose(s) for which the entity is collecting and may use or disclose the personal information**
- **the types of third parties to whom the entity may disclose the personal information**
- **if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection**
- **the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and**
- **the location of the entity's privacy policy which sets out further information.**

Proposal 8.4: Strengthen the requirement for when an APP 5 collection notice is required – that is, require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless: the individual has already been made aware of the APP 5 matters; or notification would be impossible or would involve disproportionate effort.

Currently APP 5.1 provides that:

> *"At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:*
> *(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or*
> *(b) to otherwise ensure that the individual is aware of any such matters."*

It is unclear to the AMA how Proposals 2.4, 8.2 and 8.4 achieve the objectives of obtaining genuine consent without overloading consumers with unnecessary notifications. In the case of a medical practitioner, these Proposals would require an APP 5 notice to be issued:

- when the patient first attends the practice;
- when the practitioner receives results from a pathologist, imaging provider or another practitioner to whom the patient was referred; and
- when automated information is received from MBS, PBS or a pharmacist.

The Review also states (on pages 76, 134 and 136) that:

> *"As considered in Chapter 2, consent will be required under APP 3.3 where sensitive information is inferred or generated."*
>
> *"Proposal 2.4 to amend the definition of 'collection' to provide clarity that inferred personal information is covered by the Act – would address concerns that profiling which infers personal information may not be covered by the Act. It would ensure that where profiling results in inferred sensitive information, consent to that collection of sensitive information is required."*
>
> *"Where the network infers personal information about a user, this would be defined as a 'collection' under the Act, and any inferred sensitive information would require consent."*

While these paragraphs are targeted at profiling by online platforms, they also capture any other information that is "inferred" from other information that has been collected. This suggests that every time the doctor forms an opinion based on the personal information (e.g. that the patient has low iron or cancer), this is a separate "collection" that requires an additional APP 5 notice and additional consent from the patient. This is not useful or practical.

Proposal 3.4: Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force:

The AMA does not support amending section 80P(1)(d) to give organisations a general right to disclose to a State or Territory body for a "permitted purpose" if an emergency is declared under Part VIA. This is because:

- While COVID-19 has been provided as a justification, so far, no Emergency Declaration has been made under Part VIA in relation to the COVID-19 pandemic;
- the definition of "permitted purpose" is very broad and, unless Proposal 3.3 is also adopted, there would be no ability to selectively authorise specific information sharing acts or practices of particular types of entities;
- State and Territory authorities are not required to comply with the Privacy Act; and
- the submissions cited in the Discussion Paper do not provide a complete picture of the existing avenues for disclosure.

Section 80P(1)(d) allows private sector organisations to disclose personal information to:

> *(i) an entity; or*
>
> *(ii) an entity that is directly involved in providing repatriation services, medical or other treatment, health services or financial or other humanitarian assistance services to individuals involved in the emergency or disaster; or*
>
> *(iii) a person or entity prescribed by the regulations for the purposes of this paragraph; or*
>
> *(iv) a person or entity specified by the Minister, by legislative instrument, for the purposes of this paragraph.*

Paragraphs (ii), (iii) and (iv) allow disclosure to State or Territory authorities. This is because:

- A body politic is a "person" (section 2C, *Acts Interpretation Act 1901*) so is already covered by paragraphs (iii) and (v); and
- while paragraph (ii) appears to only apply to "entities", in section 80P the term "entity" includes "persons" (see section 80P(7)). This could be emphasised by adding a note to the provision or amending section 80P(d)(ii) to replace "entity" with "person or entity".

Organisations can also share personal information with States and Territories authorities without prior consent where:

- Required by law (e.g., information about who has checked into a café which was attended by a Covid-positive case) or information about whether staff working in a hospital have been vaccinated);
- it is "necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety" and it would be unreasonable or impracticable to obtain prior consent (section 16A, item 1); or
- the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose and the secondary purpose is (directly) related to the primary purpose (APP 6.2(a)).

There is also already the capacity for organisations to disclose information to the Commonwealth and for the Commonwealth to pass the information on to the State or Territory organisations that are assisting with the response.

Consideration should also be given to requiring States and Territories that receive information under section 80P to afford it the same protection as if they were APP entities. While subsection 80P(7) applies to "persons" (including State government bodies), we expect that the designated secrecy provisions only have limited application (if any) to government bodies.

Proposal 10.2: Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- **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.**

Proposal 10.2 may have unintended consequences for medical research, particularly if the definition of "personal information" is expanded to include all information about an individual even if that individual is not identifiable. This would include both data (e.g., vitals) and images (e.g., a photo of a rash). It may also include biometric information and inferred information.

As drafted, Proposal 10.2 would not allow the child or their parents to consent to collection of the child's health information unless it was "in the best interests of that child". This concept is primarily used in Family Law and it is not clear how it would apply here. Doctors, hospitals and researchers who collect health information from a child with leukemia cannot promise that their research will provide any physical benefit to that individual child. For an older child, the child could derive some psychological benefit from knowing they are helping other sick children. However, there is no benefit to a baby personally for their health information to be collected, used or disclosed for medical research.

Proposal 10.3: Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Proposal 10.3 needs to be considered in conjunction with the other changes proposed in the Review, particularly the recommendations that:

- All unit record data be treated as personal information unless it is no longer possible to identify someone from the information (Proposal 2.5).
- Unit record data also be treated as personal information (even if it is not identifiable) if "an individual is distinguished from others or has a profile associated with a pseudonym or identifier" (page 27).
- A new inference (such as a diagnosis or research finding) be treated as a new collection for the purposes of APP 3 that requires a separate consent.
- Data not be collected about children unless it is in their best interests (Proposal 10.2).

Existing data sets would not meet these requirements and the AMA does not recommend that they apply going forward to medical research.

Proposal 10.4: Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

Proposal 10.4 would substantially reduce the circumstances in which APP 6.2(a) would apply. This change would also apply to non-sensitive information such as a person's name, address and email address, including information that is publicly available (e.g., in the electoral role or phone directory or on a company website). The practical implications of this are wide ranging. For example, in the medical context, a practitioner would not be able to use the patient's information to:

- follow up an outstanding payment; or
- provide information requested by a regulator (such as Medicare or the Medical Board),

unless:

- this was expressly stated at the time this information was originally collected; or
- the patient has subsequently provided their consent (under APP 6.1).

The Review has queried whether this change would restrict public interest research. As noted above, given that medical research is unlikely to assist a specific patient, it is not "reasonably necessary to support the primary purpose" (being treating the patient). Accordingly, Proposal 10.4 would prohibit health information from being used for medical research unless:

- only aggregate or randomised data were used (which is not feasible for medical research);
- the patient gave their express consent; or
- existing exceptions allowing research with ethics approval are maintained.

In other words, this change would substantially increase the circumstances where ethics approvals are required to conduct research.

Proposal 11.1: APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- **The collection, use or disclosure of biometric or genetic data**
- **Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.**

The Review notes (on page 154) that:

> *"Option 1 in Proposal 11.1 would require APP entities that engage in restricted practices to undertake additional organisational accountability measures to adequately identify and mitigate privacy risks in a flexible and scalable way. This could require a formal PIA depending on the circumstances. Specific record keeping requirements could also apply to enable the APP entity to demonstrate compliance with the principle of privacy by design for assessment by the Information Commissioner, if required."*

There are many instances where the above criteria may apply to health practitioners, including sole practitioners. For example, an obstetrician may collect generic information in order to assess risks of birth defects. Similarly, a physiotherapist may take a video recording of a patient's gait. Arguably all health services represent a "high privacy risk" because they collect sensitive information and health information has been a target of cyber criminals.

In short, applying these criteria generates a perverse outcome. Healthcare should not be treated as a "restricted practice" that requires special approvals or a formal privacy impact assessment.

Proposal 12.1: Introduce pro-privacy defaults on a sectorial or other specified basis

Option 2 (single click) is premised on an electronic environment where the consumer can tick boxes, receive automated notices about the consequences of opting out and change their mind later. This could work for telehealth (and appointment booking platforms), but it is harder to make this work in a medical practice that uses hard copy forms to onboard patients.

Similarly, it is not clear what Option 1 (default setting is to not consent to any activities that are not "strictly necessary for the provision of the service") would look like in practice. For example, does it mean that the default is limited to the following items?

- Use of my health information but only to the extent needed for the doctor I am seeing today to diagnose and treat me.
- Record keeping but only where required by Medicare (2 years) or in those States where this is required by law and only in hard copy.
- Billing me (but not chasing me up if I don't pay).
- Disclosure to third parties but only where required by law (e.g., a subpoena or legally binding notice to produce).

In this interpretation the patient would need to specifically tick or otherwise signify their consent to each of the following items (on the basis that they are not "strictly necessary" to provide the patient with healthcare):

- The practitioner keeping notes of the appointment (beyond the records required by Medicare) in those States where there is no express legal obligation to do so;
- administrative staff lodging a claim for an MBS or private health insurance rebate on behalf the patient;
- use of any electronic record systems that can be accessed by third parties or which involve overseas hosting;
- disclosure to accountants or debt collectors; and
- disclosure to third parties if authorised by law but not required by law. This could include disclosure to Ahpra, Medicare, PSR or the practitioner's MDO.

Would Option 1 allow a practitioner to refuse to provide the service unless the patient agrees to some or all of these items (i.e., a bundled consent)? For example, it may not be feasible to have records that are not kept on the main electronic system, or which are not accessible by all members of the practice.

In short, "strictly necessary" is unclear and potentially a high standard. A practitioner who gets it wrong (by not providing an opt out) will have interfered with the patient's privacy and potentially poisoned the validity of their consent. In our view, this increases the burden on practitioners without providing any improved privacy protection for patients. Instead, the focus should be on obtaining genuine consent from patients in relation to those items where there is a practical option to "opt out" (and hence to "opt in"). In this case, these may be:

- Using information already on My Health Record;
- recording new information to My Health Record;
- disclosure to Medicare or a private health insurer (to obtain a contribution);
- disclosure to specialists or referring doctors;
- disclosure of test results by mail, text or email or over the phone;
- disclosure to family members or other third parties; or
- participation in research projects.

A decision by the patient at the practice level to opt out (or not opt in) of participation in research projects at the practice level should not be interpreted as meaning that the patient will never be included in medical research. The practice would not provide these data (e.g., as part of Practice Incentive Program) but this should not limit the ability of medical researchers to potentially obtain the same or similar information through MBS/PBS datasets, hospital admission datasets or disease registers.

Proposal 13.1: Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16

Any requirement to obtain parental consent for all persons under 16 would mean that doctors cannot treat them without notifying their parents and obtaining their consent. This is not consistent with the age for control of My Health Record (14), getting your own Medicare card (15) or the principles in *Gillick*.

There may be circumstances where a person under 16 needs healthcare (e.g., contraceptives, morning after pill, treatment for an assault, help to quit smoking or an issue involving drugs or alcohol) but does not want to alert their parents. Currently health care professionals may choose to provide treatment if they are satisfied that the patient is *Gillick* competent. No justification has been provided in the Review for changing this.

Other unintended consequences of this change for the health sector would be:

- Support services such as headspace and KidsHelpLine would not be able to offer webchat, email and phone services to persons under 16 without establishing mechanisms for their parents to provide consent.
- An APP entity (such as a local pharmacy) could not accept a CV from a person under 16 without their parent's consent.
- Persons under 16 could not submit online applications to study aged care or allied health courses at TAFE.

An alternative approach would be to specify that a 16 year old is assumed to have capacity to consent (safe harbour) while allowing APP entities to assess capacity on an individualised basis where it is practical to do so. This could also be subject to any other specific restrictions that apply in relation to specified services, organisations or activities.

Proposal 14.1: An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

As noted above, there are some areas where 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 decide that they do not want (or no longer want):

- some types of information recorded to My Health Record; or
- their specialist to update their referring GP.

A patient can choose to end their relationship with a health practitioner at any time. This means that the health practitioner will no longer use their records to provide them with health care. However, the health practitioner must still be able to use and disclose the patient's existing records. There may also be scenarios where information is collected after the end of the relationship (e.g., where pathology results or reminders are sent to the practice).

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. In some States and Territories (e.g., NSW) there is a statutory obligation to retain records for 7 years (or for patients under 18, until the patient is 25). These time frames are also recommended by MDOs for practitioners in other jurisdictions. Patients should not be able to withdraw consent to this. This would include scenarios where these records were held in records management systems that are hosted outside Australia.

Other areas where patients should not be able to withdraw their consent (even though they are no longer receiving services) are:

- The practitioner keeping notes of the appointment (beyond the records required by Medicare) in those States where there is no express legal obligation to do so;
- administrative staff lodging a claim for bulk billed services;
- disclosure to accountants or debt collectors (e.g., where a patient has not paid the anaesthetist for a surgery that has already occurred); and
- where the practitioner needs (but is not legally required) to produce the records to respond to a negligence claim (including by the patient) or a request for information by Ahpra, Medicare, PSR or the practitioner's MDO.

Proposal 14.1 also needs to be considered in conjunction with the proposed expansion of the definition of "personal information", particularly the suggestion that information is personal information if it relates to a specific individual even if that individual is not identifiable. As noted above, this could include photographs of medical conditions. If these photographs are included in published journals or online textbooks, as written, this would allow the subject to ask the publisher (such as the Medical Journal of Australia) for that photograph to be removed (even if they consented to it at the time). The AMA is unclear whether "reasonable steps" would require that the photograph be removed from future editions of hard copy textbooks.

Proposal 15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions at 15.2, below:

- **the personal information is sensitive information**
- **the personal information relates to a child and erasure is requested by a child, parent or authorised guardian**

Unless it is de-identified, health information is always sensitive information. Accordingly, Proposal 15.1 would always apply to health care providers. For the reasons set out above in relation to Proposal 14.1, this is not appropriate for health records held by registered (or retired) health practitioners. Is this what is intended by the exception for records "required for the purposes of occupational medicine" on page 122? If so, the term "required" is too narrow as in some cases there is no express legal obligation "requiring" that these records be kept and use for this purpose.

Proposal 15: Should a right to erasure apply to personal information available online, including search results?

It is not clear how this would apply in relation to journals – such as the Medical Journal of Australia and Insight Plus – that are published online. This includes information such as author names and qualifications as at the date of publication. It is not usual practice to delete scientific articles after they have published.

The proposal that there also be a separate right to request erasure of any personal information (including non-sensitive information) that relates to a child also needs to be considered in the context of photographs of unidentifiable children with medical conditions that appear in journal articles or medical textbooks. Journals are increasingly published online. It is not practical (or desirable) to require deletion of these photographs months or years after they were published.

Proposal 16.2: The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

This proposal has been included in Chapter 16, which relates to direct marketing. However, it has broader implications. Doctors collect and use personal information about their patients for the purpose of influencing their behaviour. For example, they may weigh a patient or ask them about their diet or exercise in order to encourage them to lose weight. Similarly, they may order tests to assist the patient in making decisions about their treatment.

Under proposal 16.2, doctors would have to expressly state in APP 5 notices that they are collecting or using health information for the purpose of influencing the patient's behaviour or decisions. As noted above, it is unclear whether the doctor would need to repeat this every time they received new information about the patient (e.g., test results or a report from another specialist) or formed a new opinion about the patient.

More broadly, this obligation would apply to the AMA itself. We regularly provide information to members (either as a group or in relation to requests for advice) to assist them in making decisions or in order to influence their behaviour.

Proposal 16.3: APP entities would be required to include the following additional information in their privacy policy: whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual

This proposal raises the same issue as Proposal 16.2. As written, doctors would need to include an express statement in their privacy policies that they will use health information (including information collected from other health providers and opinions formed by the doctor) to provide health care and that as part of this they will be using that information to try and influence the patient's behaviour or decisions. This adds words but not content and further underlines the benefits of the existing principles-based approach adopted by the APPs.

Proposal 18.1: An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort

As noted in the Discussion Paper there may be circumstances where it is inappropriate to disclose the source of information. For example, the information may have been provided by a whistle-blower. In the medical context, there may also be scenarios where family members have provided information on a confidential basis. This could be for the purpose of treating a patient with mental health issues or identifying potential genetic issues. There may also be scenarios where adult children have asked a patient's doctor to consider whether the patient is still fit to drive.

Currently, a doctor can refuse to give a patient access to health information under APP 12 if:

- the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
- giving access would have an unreasonable impact on the privacy of other individuals.

These exceptions should continue to apply.

Proposal 18.3: Where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual

This proposal is not supported by the AMA. Doctors routinely receive requests under APP 12 (and equivalent provisions of State legislation) to provide copies of medical records to new practices, third parties or the patient themselves. As drafted, Proposal 18.3 would require practitioners to provide a general, possibly written, summary of medical notes, pathology results, scans and specialist reports. These documents are written for a medical audience and are not readily understandable by an ordinary reader.

Where the request is by a current patient, there may be the capacity for this general summary to be provided verbally as part of a (Medicare funded) appointment. However, as drafted, practitioners would be required to provide this summary to former patients or third parties, such as insurance companies or law firms. In some cases, these requests are made many years later, when the practitioner may have retired or died. Is the intention that the practitioner would be able to recover the costs of providing this general summary?

Question 18: Should an APP entity be required to keep personal information it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information?

It is not clear to the AMA how this would apply in relation to journals – such as the Medical Journal of Australia and Insight Plus – that are published online. This includes information such as author names and qualifications as at the date of publication. It is not usual practice to alter scientific articles after they have published. If the author wishes to correct the article, this would be attached to the article so that there is a clear record of the original and the change.

Proposal 19: What is the best approach to providing greater clarity about security requirements for APP entities?

The AMA supports the provision of further guidance to APP entities of security requirements. This could include some 'safe harbours' that set out 'gold' standards. This would provide assurance that, so long as these standards are complied with, a third-party hacking incident would not constitute an interference with privacy. The entity would still be required to comply with the notifiable data breach scheme. However, these minimum standards would not be mandatory, and entities would still have the flexibility to meet their obligations in other ways.

The AMA notes also the example given on page 146 of the Review:

> *"For example, a pharmacy or medical practice that holds sensitive personal information, such as health information and uses outsourced providers to provide cloud and other IT services. These types of APP entities would be reasonably expected to have contractual measures in place to protect sensitive personal information and more sophisticated ICT security policies and software security as opposed to a smaller entity that only holds a small amount of personal information."*

Unlike pharmacies, which are underwritten by companies like Chemist Warehouse, Sigma Healthcare, EBOS Group and Australian Pharmaceutical Industries, medical practitioners are predominantly small businesses with limited resources. Accordingly, our members would appreciate support from the Office of the Australian Information Commissioner (OAIC) or other government agencies in implementing these "more sophisticated ICT security policies and software security" and negotiating contractual measures with local and global IT vendors.

Proposal 20.1: Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

We assume that this proposal is only intended to apply to any use or disclosure under APP 6.2(a) and is not intended to apply to the other grounds for use or disclosure (in APP 6.2 or elsewhere in the Privacy Act). As amended by Proposal 10.4, APP 6.2(a) would only allow disclosure for a secondary purpose where:

- The purpose directly related to, and reasonably necessary to support the primary purpose; and
- the individual would reasonably expect the APP entity to use or disclose the information for that purpose.

However, Proposal 12.1 requires an entity to design its privacy consents on the basis that:

- Individuals can only be required to consent to activities that are "strictly necessary" to provide them with a service; and
- other uses or disclosures are only permitted if the individual "opts in" (or another exception applies).

In other words, there is no basis for an APP entity to conclude that a secondary purpose is:

- not strictly necessary for the provision of the service (and hence consent is required); but

- directly related to, and reasonably necessary to support the primary purpose; and
- something that the individual would reasonably expect the APP entity to do without obtaining a further consent.

A possible scenario would be where the APP entity fails to notify individuals of something which is necessary for it to provide the service (i.e., opt out is not feasible). Under proposal 10.4, the primary purpose would be limited to:

> *"the purpose for the original collection, as notified to the individual"*

For example, if a practice failed to expressly notify patients that letters to the practice are opened and filed by administrative staff, then arguably that would be a "secondary purpose". Similarly, it could be a secondary purpose if the practice failed to tell patients that one of the conditions of Medicare rebates is that Medicare can request information to support a claim.

In each of these cases, it is not clear what the advantage is to the individual of actively considering the secondary usage and recording it either in the practice's general records or the patient's files. Or is the intention that the practice could make a single record (for all patients) that are updating their privacy policy and APP 5 notices and/or refreshing their consents but, in the interim, the practice has determined that the secondary usage is justified by APP 6.2(a)?

Either way, this is assuming a level of understanding of the APPs that is not realistic for what are predominantly small businesses.

Proposal 22.1: Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a)

The AMA supports this amendment. However, we recommend that the prescribed list is not exhaustive given the potential for other countries to improve their privacy regulation over time.

Proposal 22.2: SCCs for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information

The AMA supports standard contractual clauses (SCCs) as long as they are not mandatory. This is because our members are not usually able to require larger entities to change their standard contracting terms.

Proposal 22.3: Remove the informed consent exception in APP 8.2(b)

The AMA supports this amendment. It is common for larger entities to include "consent" provisions in standard form contracts that are not open to negotiation or can be changed unilaterally by the provider. Practitioners have a legitimate expectation that their IT providers take responsibility for their subcontractors, including subcontractors based outside Australia.

Proposal 22.4: Include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3

The AMA recommends that entities have the option to either disclose this information in an APP 5 notice (as is currently the case) or their privacy policy. Otherwise, APP entities will need to update their privacy policy every time they enter into a new contract with a third party (e.g., a lawyer, an accountant, an IT provider or recruiter) that involves overseas disclosure.

We note also that privacy policies are generally publicly available and there may be circumstances where it would not be appropriate (e.g., for confidentiality, security or privacy reasons) to list the specific personal information that is being disclosed.

Proposal 22.5: Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines

The AMA supports this amendment. It will create greater certainty for practitioners who use cloud based medical records management systems that may involve overseas hosting.

Proposal 24.5: Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss

The AMA accepts that practices that experience data breaches should take reasonable steps to prevent future losses such as that listed on page 179: "This could include requiring the entity to pay a reputable provider for credit monitoring services to monitor whether information that is the subject of the breach has been used for identity theft or fraud for a certain time period after the incident."

However, Proposal 24.5 is not limited to notifiable data breaches (NDB). The NDB scheme only applies where serious harm (e.g., identity theft) is likely. Proposal 24.5 would apply to any interference with privacy, no matter how minor. We note also that the existing provision (section 52(1A)(c) empowers OAIC to make a declaration that the:

> *"Person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals."*

This involves proof of actual damage. Proposal 24.5 is more nebulous in that it allows OAIC to declare that:

> *"The respondent must 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."*

This is putting the onus on the organisation (which may be a sole practitioner) to identify any loss or damage could be suffered. They would need to outsource this. We note also that:

- the standard "reasonably foreseeable loss or damage" is a much lower standard than the standard under NDB both in probability (likely vs reasonably foreseeable) and quantum (serious harm vs any loss or damage).

- the wording of (c) differs from the wording of (b) and (d) in that it does not refer to "specified steps". OAIC will be in a much better position to determine what should be done, i.e., a doctor would not know what to do if OAIC made a general declaration in the terms of paragraph (c).

An alternative formulation would be:

> *(c) a declaration that the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals*
>
> *(ca) A declaration that the respondent must take specified steps (which must be reasonable) within a specified period to mitigate any serious harm that those individuals are likely to suffer in the future.*

Proposal 24.1: Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses, including … A new mid-tier civil penalty provision for any interference with privacy

Proposal 24.1 needs to be considered in conjunction with the other changes proposed in the Review. These changes involve introducing new minimum requirements that must be complied with whenever collecting, using, disclosing or storing health information. As highlighted above, the proposed changes are not framed with medical practices in mind and often do not make sense in the context of medical practices.

Any breach of these requirements – no matter how minor – constitutes an "interference with privacy" and hence would be subject to this new regime.

Proposal 24.7: Introduce an industry funding model similar to ASIC's incorporating... a statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment

This Proposal is premised on identifying "high risk privacy industries". As noted above, arguably all health services represent a "high privacy risk". However, they are predominantly small businesses, and no evidence has been provided that OAIC is receiving excessive complaints relating to medical practitioners/practices. Accordingly, these criteria should not be used to impose a "privacy tax" on medical practitioners/practices who provide services directly to patients, including via telehealth.

By contrast, under the UK model, medical practices pay between 40 and 60 pounds per year depending on staff numbers and turnover. However, like television tax in the UK, this is a broad-based tax that is paid by most businesses that collect personal information.

Proposal 24.9: Alternative regulatory models

The AMA also has some concerns about any requirement that medical practitioners/practices pay a fee every time a complaint is made to OAIC (akin to fees paid by telcos to the Telecommunications Ombudsman). For example, the AMA regularly answers questions from the public about access to medical records. Some of these relate to situations where medical practices have not fully understood their obligations. However, many involve members of the

public who erroneously believe that they are entitled to access their medical records free of charge.

As is the case in the telecommunications industry, there may be scope to refer privacy complaints to another regulator. For example, the Commonwealth Ombudsman – private health insurance already handles confidentiality and privacy complaints about private health insurers.[5] However, we do not consider it appropriate to require all private practitioners to join an industry scheme.

Proposal 25.1: Create a direct right of action

The AMA does not support a direct right of action or the proposed provision for class actions. If a right of direct action is introduced:

- there should be a gateway of the type proposed in Proposal 25.1; and
- it should be limited to serious or repeated breaches of privacy.

Proposal 26: Statutory Tort

The AMA does not support the establishment of a statutory tort.

Proposal 28.3: Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues:

The AMA's main concern is laws that regulate the collection, use, disclosure and access obligations for private sector health practitioners (i.e., organisations), particularly:

- My Health Record.
- Health Records and Information Privacy Act 2002 (NSW).
- Health Records Act 2001 (VIC).
- Health Records (Privacy and Access) Act 1997 (ACT).

The key issues are:

- **Notifiable Data Breaches** – This is discussed in the ADHA submission[6] and on pages 157 and 198 of the Discussion Paper.
- **Provisions relating to access by patients and third parties to medical records held by private sector practitioners** – The fees and grounds for refusal vary depending on whether the request was made under the Privacy Act or State laws.
- **Records of deceased persons** – This is not regulated by the Privacy Act (unless it is also genetic information of a living person). However, health records held by private sector organisations are regulated by the MHR and State legislation in Victoria, NSW and the ACT. This legislation has different rules about who is authorised to request access.
- **Transfer of records on closure or sale of business** – There are different approaches in the Victoria, NSW and ACT legislation. The ACT legislation is the most practical as it requires

[5] Commonwealth Ombudsman, Private Health Insurance Quarterly Report 1 July–30 September 2021
[6] Australian Government Australian Digital Health Agency 2020

practices to tell ACT Health (who pass this information onto the ACT Health Services Commissioner) where records will be stored.

The AMA also reiterates that the amendments to the Privacy Act need to align with the *Data Availability and Transparency Bill* as it will also regulate research (albeit only for Commonwealth government data sets).

24 JANUARY 2022

Contact
Nicholas Elmitt
Medical Practice Policy Manager
Australian Medical Association
Ph: (02) 6270 5400
E: nelmitt@ama.com.au