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

Privacy Act Review

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

privacyactreview@ag.gov.au

Thank you for providing AMA with an opportunity to comment on the *Privacy Act 1988* Review - Issues Paper.

We note that the review is seeking answers on 68 questions. In the time available and noting this is the first submission in a series of planned consultations, our response focuses on questions that are of particular interest to our members.

Question 1 – Should the objects outlined in section 2A of the Privacy Act be changed? If so, what changes should be made and why?

In the AMA's view, the current principle-based approach in section 2A of the Privacy Act achieves the flexibility needed for a single Act to regulate consumer privacy across diverse organisations.

We note that "business" in this context is not necessarily a large commercial organisation. It also includes medical practitioners who provide healthcare. Many of these organisations are sole practitioners or small businesses.

Any changes to the Privacy Act should not impose additional privacy regulation on medical practices as they already are required to adhere to strong privacy positive practices in the process of providing healthcare.

Questions 3, 35 and 36 – Inferred personal information

As noted in the Issues Paper, the existing definition of "personal information" is intentionally broad. In many cases "inferred information" will already fall within the definition of personal information and, in some cases, "sensitive information".

Most of the personal information handled by our members is "sensitive information" but it is obtained directly from the patient during an individual patient consultation or provided by another healthcare provider involved in the healthcare of the same patient, or derived from test

results the patient agrees to. These actions are already well covered by the existing provisions in the Privacy Act.

For example, a GP may collect information from the patient, a pathologist and a PET scan. Together that information may allow the GP to infer a new piece of personal information, namely that the patient is likely to have cancer. GPs treat this diagnosis as sensitive information. However, they would not treat this is a new collection that requires a new APP 5 notice or ask themselves whether this new piece of sensitive information should have been collected directly from the patient (APP 3.3).

In other words, the AMA does not consider that amendments are required to the definition of "personal information" to address inferred information and is concerned that an over prescriptive approach to inferred information could have substantial repercussions for doctors. Similarly, we do not consider any changes are required to the Privacy Act to protect against the misuse of sensitive information by health practitioners.

Question 4 – Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

The AMA supports strong protections to ensure de-identified data is not released in a format that, when combined with other data, can reasonably become identifiable (unless the patient has consented to this). However, the AMA also supports the availability of non-identifiable data for clinical research. In other words, while privacy is clearly important, a practicable path to the use of data in clinical audit and clinical research offers substantial benefit in auditing and improving health outcomes in an Australian-specific context. For example, GPs currently provide de-identified data as part of the Practice Incentive Program (PIP) Quality Indicators (QI). The purpose of the program is to improve the quality of care for all Australians.

Currently the primary pathway for medical research is section 16B (Permitted health situations). As noted on page 85, the interim National Data Commissioner has also recently released a *Data Availability and Transparency Bill*. This Bill is intended to provide additional pathways for the use of de-identified data by appropriate persons for research and other appropriate purposes. The AMA has provided submissions in relation to this Bill which emphasise the need for de-identification processes to performed by trained personnel and in accordance with existing best practice.

Given this background, the AMA is concerned that:

- adding additional de-identification or anonymisation requirements into the Privacy Act; and/ or
- expanding the Privacy Act so that it covers de-identified data,

has the potential to further complicate the legislative framework and stymie legitimate research. For example, for a GP to "irreversibly treat data so that no individual can be identified, including by the holders of the data" (page 20) they would need to know what data is held by the recipients of the data (in this case Primary Health Networks and the Australian Institute of Health and Welfare who are trusted data users). We expect that this kind of

anonymisation for data provided to trusted users, would also reduce the efficacy of the data for conducting research.

Question 5 – Expansion of the definition of 'personal information' to include information about deceased persons

Any proposal to expand the Privacy Act to deceased people needs to have regard to health records, including My Health Record. We regularly receive requests for advice from both doctors and relatives about access to medical records for deceased patients.

While the Privacy Act generally does not apply to deceased persons, doctors generally treat the information of deceased patients with the same respect as for living patients. Some State legislation (such as Victoria and ACT) sets out who has authority to request copies of records of deceased patients. In other jurisdictions, it is less clear who has authority to access these records.

Access to medical records of deceased persons is an important practical issue for doctors as they are subject to an ethical obligation to explain a patient's death to relatives unless the patient would not have wanted this. Paragraph 3.13 of the Ahpra Code of Practice relevantly provides that:

> *4.13.10 Communicating bad news to patients and their families in the most appropriate way and providing support for them while they deal with this information.*
>
> *4.13.11 When your patient dies, being willing to explain, to the best of your knowledge, the circumstances of the death to appropriate members of the patient's family and carers, unless you know the patient would have objected.*
>
> *4.13.12 Sensitively discussing and encouraging organ and tissue donation with the patient's family, when appropriate and consistent with legislation and accepted protocols.*

Relatives may also want access to a deceased patient's medical records:

- as evidence (eg, where a person died as a result of a workplace injury or a motor vehicle accident or they suspect there was medical negligence);
- to make an insurance or superannuation claim;
- to understand their own health better (eg, where there is a family history of breast cancer); or
- to help them process the situation (eg, a suicide or unexpected death).

Information about cause of death is also very relevant to medical research, education and quality improvement.

We note also that, in addition to issues about who can give consent, where a patient has died, there are very limited circumstances where disclosure of their records will fall within the existing permitted health situations (section 16B). Similarly, the AMA has previously recommended that *My Health Record Act 2002* be amended to clarify the ability of medical

practitioners to access the My Health Record of deceased patients, including in circumstances where the medical practitioner is not aware that the patient has died.

Question 5 (continued) – Other changes to the definition of personal information

For completeness, we suggest that the definition of "sensitive information" be amended to remove the reference to membership of a professional association. Membership of a professional association, such as the AMA, Engineers Australia or the Law Society, is personal information but is not in the same category as the other types of information that are sensitive information.

Question 6 – Is the framework of the Act effective in providing flexibility to cater for a wide variety of entities, acts and practices, while ensuring sufficient clarity about protections and obligations?

In our view, the APPs strike a good balance and allow different approaches to be taken in different circumstances.

The OAIC has prepared a useful guide for health service providers on how the APPs apply in the health space. See https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-health-privacy/guide-to-health-privacy.pdf

Questions 7 to 12 – Small business exemption

The small business exemption is generally not relevant to our members as it does not apply to organisations that provide a health service.

However, it can be relevant to our members where they use outsourced providers to provide IT and other services. Currently section 6D(4)(b) provides that an organisation will not be a small business if it "provides a health service to another individual and holds any health information except in an employee record". This generally would not include companies that provide cloud and other IT services to medical practices as they do not provide health services and any records are held for the medical practice. This means that medical practices (which are often themselves small businesses) are responsible for:

- checking whether these providers have a turnover over $3 million; and
- if not, ensuring that their contracts with these providers require compliance with the Privacy Act.

The AMA would support a direct obligation on these small IT businesses to comply with the Privacy Act when they are engaged under contract to provide IT services to a healthcare provider. This is because these provides have often have the technical capacity and capacity to access to sensitive health data (notwithstanding that the contract may prohibit or regulate this) and the healthcare provider is relying on these providers to support its own compliance with the Privacy Act.

Questions 13 to 15 – Employee records exemption

Our members are not seeking any changes to the employee records exemption.

Questions 20 to 25 – Improving awareness of relevant matters

The AMA does not support changes to the Privacy Act that that would require all APP entities to use standardised words or icons to notify individuals about how APP entities use personal information. This one-size-fits-all approach would impose an additional administrative burden on medical practitioners without providing any significant benefit to patients.

All registered healthcare providers are already subject to the **Medical Board Code of Conduct** which sets a clear requirement on all registered doctors to protect the confidentiality of patient information and ensure sharing of information about patients is consistent with privacy laws, including consent requirements.

Question 23 – Third party collections

Third party collections are very common in the health space. For example, a GP will provide personal information about a patient to a specialist as part of a referral. The specialist will not usually send their own APP 5 notice to the patient (as the patient will expect their personal information will be provided to the specialist). However, the specialist:

- will only use the information for the purpose for which it was provided (APP 6); and
- is collecting sensitive information from a person other than the patient in order to provide a health service to them (section 16B(1)).

As noted by OAIC (Chapter 3 of https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-health-privacy/guide-to-health-privacy.pdf), the specialist may also use the patient's information for related purposes, such as billing. This is particularly applicable where a specialist (eg an anesthetist) has only had limited interaction with the patient.

Questions 26 to 29 – Consent to collection, use and disclosure of personal information

Our members are not seeking any changes to the existing consent framework.

The AMA does not support a one-size-fits-all approach to ensuring that any consent given by patients (and their families where relevant) to the collection, use and disclosure of information is freely given and informed.

It is not practical for patients to be required to separately consent to each purpose for which an entity collects, uses and discloses information. As noted above, patients usually provide implied consent for information to be collected by a medical practice (or hospital) and provided to other members of their care team. This consent may be withdrawn. Doctors may also rely on section 16B (Permitted health situations) to collect information from patients about themselves and their families in order to provide health care.

We appreciate that there may be some circumstances where suppliers are inappropriately bundling consents. However, we do not consider additional regulation is the solution. Who

decides what personal information is "necessary" for providing a relevant product or service? Will the provider be forced to provide the individual with the product or service?

Subject to anti-discrimination and competition laws, doctors – like any other service provider – can choose not to provide a service. This may, include, but is not limited to, circumstances where a patient refuses to consent to their personal information being collected, used or disclosed on the basis that the patient (or another regulator such as OAIC or the ACCC) does not consider that the information is "necessary" for the doctor to provide health care.

Question 30 – Managing consent fatigue

The AMA notes that requiring more frequent and detailed consents has the real potential to lead to consent fatigue without any increased protections to individuals' privacy.

As discussed further below, the AMA supports the approach taken by OAIC in relation to data breach notification whereby the primary focus is on mitigation and notification only occurs where the breach is still likely to result in serious harm.

Similarly, the focus of the consent process should not be on creating additional paperwork.

Question 31 – Exceptions to the requirement to obtain consent

Our members are generally not seeking any changes to the current general permitted situations and general health situations. However, we note for completeness that Permitted General Situation 4 is limited to:

> *"The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim."*

While our members are required by law to comply with a Notice to Produce issued under section 129AAD of the *Health Insurance Act 1973*, the MBS compliance division of the Department of Health usually only issues a formal Notice to Produce where a practitioner has failed to respond to the Department's initial letter. The initial letter will usually:

- advise the practitioner of the concern that has given rise to the compliance action; and
- ask them to provide evidence that they have met the requirements of the items being audited. This evidence is usually in the form of some documentation.

Practitioners are not required by law to comply with these letters. Accordingly, we have previously warned practitioners that they may be non-compliant with APP 6 if they provide any documentation containing patient information prior to the Department issuing a Notice to Produce. Similar considerations apply if practitioners provide information voluntarily as part of an initial investigation by Professional Services Review (PSR) or Ahpra.

Potential solutions would be for:

- the *Health Insurance Act* 1973 or other primary legislation to authorise practitioners to provide personal information to the Department as part of an informal investigation; and/ or
- Permitted General Situation 4 was not limited to defence of legal or equitable claims. For example, it could be extended to responding to investigations or requests by regulators.

Question 32 – Pro-consumer defaults

We understand that the ACCC has recommended that, because many users want digital platforms to only collect information needed to provide their products or services, default settings enabling data processing for a purpose other than the performance of a contract should be pre-selected to 'off'.

Prior to COVID-19 digital platforms (such as HealthEngine) were primarily used to book medical services, with only a small number of providers using digital platforms to provide health service, such as online medical certificate services.

However, since during COVID-19 there was increasing use of digital platforms to provide health services and MBS rebates were extended to tele-health services. In these circumstances, health information is not collected solely to "perform a contract". For example:

- Information about PBS and MBS claims will be provided to the government.
- General practitioners provide de-identified data to Primary Health Networks as part of quality improvement programs.
- De-identified data may be used as part of medical research subject to ethics approvals.
- Doctors may be legally required to report patient information (eg about communicable disease or suspected child abuse) to State or Territory authorities.
- Doctors may also be ethically required to notify third parties where a patient is at risk of harming themselves or others.

As noted above, there may be circumstances where practitioners may be required (or requested) to provide patient information to Chief Executive Medicare, the Medical Board or other regulators.

Question 33 – Obtaining consent from children

Privacy consents in relation to children is an important issue in the health space and there is a need to adopt a more consistent approach to the age of consent.

The Privacy Act currently does not specify an age after which individuals can make their own privacy decisions. This means that APP entities need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent. OAIC has stated (https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#consent) that:

B.58 If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

However, lower ages are used in other contexts. For example:

- Under the *My Health Records Act*, once a child turns 14 years of age, the child may take responsibility for their own MHR and all Authorised Representatives are automatically removed.
- Medicare requires 14 year olds to sign any request for access to their Medicare data. (This is in addition to their parent's signature.) (See form at https://www.humanservices.gov.au/individuals/forms/ms031)
- In the ACT, a "child" is defined as under 12 and a "young person" is 12 to 17 (inclusive).
- Facebook allows children aged 13 or over to establish Facebook pages.
- The EU privacy changes allow member states to require Facebook etc to get parental consent (as well as the child's consent) for children aged 13, 14 or 15 (http://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent). (The implication is that 16 years do not need parental consent and persons under 13 cannot give consent.)

Our members also need to consider privacy consents for minors in conjunction with other legal principles. For example:

- While a 14 year old may control their own My Health Record, they may not be able to consent to a medical procedure.
- A minor lacks legal capacity to make contracts that are not for their benefit.
- We regularly receive queries about the rights of divorced or separated parents to access their children's medical records.
- Doctors need to exercise judgement about disclosing children's medical records to non-custodian parents in situations where there may be abuse or domestic violence.

Given this complexity we are concerned about any proposal to adopt a one-size-fits-all approach to how APP entities seek consent from children, including any requirement that in all cases "consent to collect the personal information of children by entities must be obtained from the child's guardian" (page 44). This is particularly the case where a minor is using a digital platform to provide confidential health care (such as contraceptive advice).

Question 38 – Requirement to refresh consent

The AMA does not support a formal one-size-fits-all requirement to refresh an individual's consent on a regular basis. Doctors are primarily small businesses. This requirement would be administratively burdensome for doctors and provide minimal additional protections for patients.

It is also unclear how this requirement would apply where – as is commonly the case for a medical practice – the APP entity is not required to seek written consent.

As discussed further below, there are also situations where records are held for a long period (eg, best practice is for children's records to be retained until the patient turns 25) or a practice changes hands, and it is not practicable to refresh patient consents.

Question 39 – Withdrawal of consent

Doctors already allow patients to withdraw consent in some circumstances. For example, a patient may advise a doctor that they no longer want information shared with other members of their care team. Children may also advise doctors that they no longer want information shared with their parents. A patient can also control who has access to their My Health Record.

However, as discussed further below, a patient should not have the ability to insist that a doctor delete all personal information held by the doctor in relation to them. This is because:

- The intellectual property in the records is not owned by the patient.
- In addition to any statutory obligations to maintain records, doctors need to maintain records for ethical and insurance purposes.

Similarly, where a patient (or their parent) has given their consent to personal information about them (eg, a photograph) being used in a study or published article, it may be impossible or impracticable for that information to be deleted.

Question 40 – Acts or practices that are prohibited regardless of consent

The AMA has concerns about any proposals that do not respect the right of an individuals to choose what they do and do not wish to consent to. As is the case for *My Health Records*, these kinds of paternalistic restrictions may have unintended consequences.

One alternative to a prohibition is additional layers of protection. For example, the AMA is supportive of proposals by the interim National Data Commissioner that some activities be subject to additional safeguards, even if individuals have signed consent forms (page 21 of https://www.datacommissioner.gov.au/sites/default/files/2020-09/DAT%20Bill%202020%20exposure%20draft%20Consultation%20Paper%20Final_0.pdf)

Question 42 – Regulating use and disclosure

In the AMA's view, the APPs (particularly APP 6) already adequately regulate the uses and disclosures of personal information.

As noted above, the OAIC has prepared a useful guide for health service providers on how the APPs apply in the health space. See https://www.oaic.gov.au/assets/privacy/guidance-and-advice/guide-to-health-privacy/guide-to-health-privacy.pdf

The AMA does not consider that any changes are required to these provisions.

Question 43 – Security

In our view the security requirements in APP 11.1 are reasonable and appropriate to protect the personal information of individuals. As noted on page 50, APP 11.1 is also scalable to reflect the entity's 'size, resources, the complexity of its operations and its business model'.

We have received number of queries from members, particularly during COVID, about the use of email and cloud-based systems. While OAIC has produced a guide (https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/), this is a rapidly changing area and further clarification about what is "reasonable" having regard to COVID-19 would be valuable for our members.

Questions 44, 46 and 47 – Retention and right of erasure

The AMA does not consider that the Privacy Act should impose greater requirements on APP entities to destroy or de-identify personal information that they hold. Similarly, the AMA does not support a right to erasure of medical records.

While any obligation to destroy, de-identify or, where requested, erase personal information would presumably be subject to any overriding legal obligation to keep records, there is currently no clear national obligation to keep medical records for a particular period.

In some State and Territories, doctors are subject to obligations to keep medical records. However, this is not consistent. Doctors are also subject to ethical obligations (eg https://www.medicalboard.gov.au/codes-guidelines-policies/code-of-conduct.aspx and codes of practice for some Colleges). Insurers also recommend that medical practitioners retain medical records for 7 years (or, if the patient is a child, until the patient turns 25). This is consistent with APP 11.2 (which allows the information to be retained if it is needed for any purpose for which it may be used or disclosed by the entity under the APPs). However, it generally does not amount to a legal obligation to retain records.

Question 45 – Access, quality and correction

The AMA does not consider any changes are required to the access, quality and correction requirements in APP 10, 12 and 13.

Question 48 – Overseas data flows

APP 8 and section 16C are complicated and it is likely that most APP entities and individuals do not fully understand the current accountability regime.

Historically doctors, hospitals and aged care facilities stored medical records in hard copy onsite. More recently cloud-based practice management systems and records management systems have become common place. This has been particularly useful during COVID as it has allowed doctors to continue to provide full services. However, patients and practitioners may not always be aware where data is stored or what unilateral rights the supplier has to change

where data is stored. Similarly, the media has raised concerns that sign in applications used by employers during COVID-19 do not always require that data be stored in Australia or another country with similar privacy protections.

That said, the existing regime does strike a balance between the rights of individuals and the obligations of APP entities in that:

- It does not prohibit cross-borders disclosures; but
- It makes APP entities responsible for breaches by the overseas entity unless an exception (such as informed consent or adequate privacy regime) applies.

The AMA is not seeking any changes to this balance.

Questions 50 and 51 – CBPR or domestic privacy certification scheme

The AMA does not support a mandatory certification scheme.

Question 52 – GDPR

GDPR has had two main impacts on the operation of the AMA itself.

First, the AMA has needed to establish procedures to remove members who it is aware are residing in the EU (eg, as part of a sabbatical) from automated email services (eg to send newsletters) given that these services can record information about when emails were opened. This may constitute monitoring of the behaviour of persons in the EU.

Secondly, global suppliers have required that the AMA agree to additional terms required to support their compliance with GDPR. This will also be an issue for practices that use global solutions for practice management, billing, IT or records management. This process may be simpler if Australia's laws were recognised as adequate by the European Commission.

Questions 53 to 62 – Enforcement powers under the Privacy Act and role of the OAIC

Our members are not seeking any changes to the existing remedies or the enforcement mechanisms.

In our view, the existing enforcement provisions – particularly the ability of individuals to complain to OAIC and for OAIC to determine that the individual should be compensated – provide adequate incentive for APP entities to comply with their obligations. In our experience, our members are very conscious of their obligations to keep patient information confidential and do not need additional "incentives" to comply with the Privacy Act.

In our view, a direct right of action or a statutory tort would encourage US-style litigation and, in the case of doctors, potentially increase insurance premiums. It would also result in entities adopting a more adversarial approach to complaints and is likely to increase the time frame for resolving complaints. As noted on page 63, currently the average time to finalise complaints is only 4.4 months.

Questions 63 to 65 – Notifiable Data Breaches scheme

The AMA has previously highlighted the difference between the notifiable data breach scheme and the obligations of healthcare providers under the *My Health Records Act 2012*. These discrepancies will become more significant as take up of My Health Record increases.

Specifically, section 75 provides that a healthcare provider organisation must notify ADHA (in its capacity as System Operator) and OAIC as soon as practicable after becoming aware that:

- a person has, or may have, contravened the Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record; or
- an event or circumstances may have occurred or arisen that may compromise, has compromised or may have compromised, the security or integrity of the MHR system.

If there is a reasonable likelihood that the issue might be serious for at least one healthcare recipient, the healthcare provider organisation must ask ADHA (in its capacity as System Operator) to notify all healthcare recipients that would be affected.

These obligations are in addition to the general obligations that apply to medical practitioners under the notifiable data breach scheme. As noted on page 76, it requires notification to OAIC and affected individuals where unauthorised access or disclosure:

- is likely to result in serious harm to one or more individuals, and
- the organisation has not been able to prevent the likely risk of serious harm with remedial action.

The AMA has previously recommended amendments be made to the *My Health Records Act* to align the data breach provisions with the data breach requirements in the Privacy Act.

This change would increase clarity and efficiencies for health care providers who would no longer need to run two different data breach reporting systems within their practice. The change would also reduce the duplication of effort needed in the OAIC to oversee two different data breach schemes without undermining the overall protections of patient privacy or the standard of health data security for information stored in the MHR.

Questions 66 to 68 – Interaction between the Act and other regulatory schemes

The AMA notes that the government is also proposing a new *Data Availability and Transparency Bill* that will override provisions of the Privacy Act. It is important that any change to the Privacy Act have regard to this Bill.

As noted at https://www.oaic.gov.au/privacy/privacy-in-your-state/, there is also legislation in most States and Territories that regulates health records. Any changes to the Privacy Act should also have regard to this legislation. As noted above, currently State and Territory legislation

does not adopt a consistent approach to the retention of medical records. Other areas of inconsistency that impact on our members include:

- Inconsistent approaches to deceased persons, including inconsistent approaches to requests for access to records of deceased persons.
- Inconsistent approaches to notifying patients and regulators of changes in the arrangements for holding records (eg, as part of a sale of a practice or retirement of a practitioner).
- Different maximum fees for providing patients or third parties with copies of health records depending on whether the request is made under the Privacy Act or State legislation.

Thank you for the opportunity to comment on the *Privacy Act 1988* review Issues Paper. The AMA looks forward to participating in the next steps of this review.

8 DECEMBER 2020