Review of the *Privacy Act 1988*

Attorney-General's Department

December 2020

Submission by the Commonwealth Department of Health

1. Introduction

This document contains the Commonwealth Department of Health's (**the department**) responses to questions set out in the Issues Paper dated October 2020, distributed by the Commonwealth Attorney-General's Department.

The department has undertaken an internal consultation process in relation to the Review of the *Privacy Act 1988* (**the Review**) involving a number of key business areas within the department that engage with the *Privacy Act 1988* (**Privacy Act**). The following submission sets out the department's views in relation the Review, taking into account the internal consultations undertaken. The submission is complemented by a number of specific examples in the context of the department's work in the Genomics space, set out in the table at Attachment 1.

2. Summary

- The department welcomes any appropriate measures aimed at balancing the needs and rights of individuals with the reduction of regulatory burden on Australian Privacy Principle (APP) entities.
- In particular, the department supports the simplification of notice requirements under APP 5 and the provision of greater guidance for agencies around notification, including standardised frameworks of notice, standard forms of words and other comparable measures to ensure a consistent approach among APP entities.
- Further, given the increasing reliance on remote data storage solutions such as the use of off-shore cloud services, the department encourages the Review to ensure the requirements of APP 8 continue to be appropriate in light of the expanding use of remote data storage solutions.
- The department is also supportive of any appropriate measures that increase jurisdictional consistency in terms of harmonising state and territory privacy regimes with the regulatory framework at the Commonwealth level.
- The department also encourages the Review to explore the definition of 'holds' in the context of APP entities' arrangements with contracted service providers (whereby data storage/hosting functions are outsourced to third parties), with a view to developing enhanced guidance on the issue.

3. Definition of personal information

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

a. For data to be considered 'de-identified', the risk of re-identification in the relevant release context must be very low.[1] This is a complex area for data custodians, particularly given the burgeoning demand for access to public sector data at very granular levels, and for linkage with other datasets.

b. The department notes that while the OAIC has published guidance materials on de-identification, data custodians may still need to seek specialist expertise in

1 See for example, definition of 'de-identified' in s 6(1) of the Privacy Act, APP 11.2 and paragraphs B.59 – B.62, APP Guidelines, see page 3, OAIC De-identification and the Privacy Act.

order to be satisfied that the likelihood of re-identification is low, particularly in light of advances in data analytic technologies.

c. The department is of the view that any changes in the Privacy Act that require additional protections in relation to de-identified, anonymised and pseudonymised information as flagged in Question 4, will need to be supported by appropriate guidance and expertise in order for implementation to be effective.

d. The department notes the challenges associated with determining the scope of 'personal information' as it relates to genomic information.[2] Genomic information will only fall within the scope of the Privacy Act if it meets the definition of personal information in s 6(1) of the Privacy Act, which can be challenging particularly in the context of data sharing and linkage activities necessary for genomics.

e. There is uncertainty and inconsistency in the application of the current test as to whether genomic information is 'about' an individual who is 'reasonably identifiable', in which case it falls within scope of Privacy Act. It is difficult to assess when genomic information may render a person reasonably identifiable, particularly as data moves between different collections with different data linkage possibilities.

f. The current definition of personal information does not indicate the extent to which account should be taken of all objective factors (for example, time, cost and technology) that can contribute to determining whether genomic information is 'reasonably identifiable' for the purposes of s 6(1) of the Privacy Act.

g. Such lack of clarity is likely to present a barrier to the uptake of clinical genomic research and services, as individuals may be unwilling to share their genomic information.

h. The department would support any appropriate measures aimed at clarifying how the term 'reasonably identifiable' is to be understood in practice in relation to genomic information (including the extent to which account should be taken of all objective factors, such as the costs of and the amount of time required for identification, the available technology at the time of the processing, and the possibility of technological developments).

i. More broadly, the department notes that any changes to the definition of 'personal information' set out in s 6(1) of the Privacy Act will have flow-on effects to other Acts which rely on this definition, particularly in the context of secrecy and data matching provisions.[3]

j. This is especially the case should the definition of 'personal information' be changed to capture technical data types or 'inferred personal information'.

k. Further guidance on this matter would assist the department to avoid inadvertent breaches where lawful activities may be affected by a revised definition such as

2 Genomics refers to both the study of single genes (genetics) and the study of an individual's entire genetic makeup (genome) and how it interacts with environmental or non-genetic factors. The term genomic information refers to sequenced DNA that can be in the form of raw data derived from sequencing, a person's genome in whole or in part, or individual DNA variations as well as, associated metadata and clinical information to support genomic interpretation.

3 See, for example: s 86-1(b)(i) of the *Aged Care Act 1997*; s 124ZR of the *Health Insurance Act 1973*; ss 132F(2)(d), (e) of the *National Health Act 1953*.

the routine disclosure of 'de-identified' information, or technical manipulation of data for compliance or research purposes (which currently do not use 'personal information' as defined in the Privacy Act but involve aggregating, linking or matching data from different sources).

4. Flexibility of the APPs in regulating and protecting privacy

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?

a. The department considers the current framework and its reliance on consent and notification provides an appropriate balance of flexibility for APP entities through the availability of relevant exceptions with necessary and sufficient protections for individuals.

b. However, the department would strongly support revisions to the framework for notification and consent in order to provide a greater degree of guidance and, where possible, templates to assist with standardisation and consistency in order to reduce the burden on APP entities while helping to manage consent fatigue among individuals.

c. Further, the department would welcome increased clarity and greater guidance around the issue of the 'holding', 'collection', 'use' and 'disclosure' of personal information in the context of arrangements with service providers that have been engaged by agencies under contract.[4]

d. There are an increasing number of circumstances in which APP entities outsource data storage functions to contracted service providers for the purpose of facilitating hosting and maintenance arrangements, including cloud storage arrangements.

e. The department would welcome greater clarity where a contracted service provider's (including cloud services providers) role is limited to providing the IT infrastructure on which personal information is stored. Specifically, further clarity both in the Privacy Act and in guidance on the relevant APP entity's and the contracted service provider's APP obligations would be helpful.

5. Notice of collection of personal information: Improving awareness of relevant matters

21. What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

a. The department notes the increasing complexity of notices aimed at making individuals aware of relevant APP 5 matters and welcomes any appropriate measures aimed at simplifying the notice process for individuals while reducing the regulatory burden on APP entities.

b. There are currently up to ten different requirements that could be included in APP 5 notices. The department would be broadly supportive of appropriate

4 We note that there is some guidance available with respect to the question of when an entity is deemed to be 'holding', 'collecting', 'using' and 'disclosing' personal information in the APP Guidelines, see in particular Chapter B. See also B.144.

measures to simplify this process, including additional guidance about the scope of APP 5 notices, the role of overarching privacy notices in making individuals aware of APP 5 matters and the development of a standard form of words to assist APP entities in complying with APP 5 obligations.

c. In addition, the department would further support any appropriate measures that assist in clarifying how the primary purpose of collection should be interpreted, particularly where there could be multiple purposes for which personal information is being collected (that is, can there be more than one primary purpose?).

d. Clarity around this issue would be helpful in circumstances where the reasons for the collection, use or disclosure of personal information may cause distress to individuals, for example where the department is handling personal information for the purposes of corresponding or communicating with individuals in relation to deceased relatives in an aged care setting.

e. A similar degree of clarity around the definition of 'routine disclosures' would also assist in providing clarity for individuals while reducing regulatory burden on agencies.

f. The department also notes the potential confusion that arises through the need to address APP 8 in collection notices through the use of terms such as 'unlikely to disclose information to an overseas recipient'. This issue is explored further as part of the discussion under Part 14 below.

6. Notice of Collection of Personal Information: Limiting information burden

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

a. The department welcomes any appropriate measures aimed at simplifying the notification process relevant to APP 5, in particular the development of a standardised framework of notice.

b. The development of a standardised framework of notice would benefit APP entities in minimising regulatory burden while at the same time providing increased clarity to individuals by ensuring consistency in the manner in which APP entities seek to discharge their APP 5 obligations.

7. Consent to collection and use and disclosure of personal information

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

a. The department notes the potential benefits of requiring consent in relation to each purpose of collection, use or disclosure. However, the department also notes the potential challenges that may arise under a more stringent consent framework.

b. Requirements to obtain more specific and explicit consent in relation to the purposes for which information is collected, used or disclosed would provide the department with greater immediate clarity around obligations for the handling of personal information.

c. Such requirements may have positive impacts in terms of lowering risks around APP entities' compliance with APP 6 through reducing the need to identify and subsequently rely on related (or directly related) secondary purposes for uses and disclosures of personal information.

d. However, the department notes that the development of an overly stringent regime in terms of consent to each individual purpose may in some instances be unreasonable given the scope of potential uses and disclosures that would currently be deemed to be a related (or directly related) secondary purpose (and the difficulties in anticipating all secondary uses or disclosures at the time of collection).

e. The ability to use or disclose personal information for secondary purposes unforeseen at the time of collection provides significant benefit to both Government and the Australian public by, for example, facilitating continuous improvement and evaluation of policy implementation and reducing the risk of individuals being disadvantaged in service delivery by not having provided the appropriate consent. The department is cognisant of the need to guard against function creep while at the same time offering some measure of flexibility with respect to unforeseen but beneficial secondary purpose uses or disclosures.

f. For example, the department manages multiple requests for access to departmental datasets for data linkage, including requests from researchers who argue that it is unreasonable or impracticable to obtain consent, or where they wish to pursue an 'opt out' consent model.

g. The department also notes an increasing requirement for enduring or longitudinal datasets where it can be difficult to anticipate future uses of the data, or to maintain contact with individuals over extended periods of time. The department considers there would be benefits in provide guidance for researchers in setting up enduring or longitudinal studies to ensure that consent and withdrawal of consent are adequately considered.

h. The department is also concerned the risk of consent fatigue will increase if there are multiple collections, uses and disclosures by various agencies. For example, in the context of statutory appointments to committees where the department collects information which is then disclosed to and used by different entities, both the burden of obtaining multiple consents and the risk of consent fatigue are likely to increase significantly.

i. The department is also of the view that further to the legislation itself, there could be significant benefit in providing greater guidance around the notion of 'reasonable expectation' where personal information is used or disclosed for secondary purposes.[5] While there is currently some guidance material published by the OAIC in the form of a Frequently Asked Questions document and examples provided in the APP Guidelines,[6] the department would welcome more specific guidance listing examples of reasonable expectations which would be included as part of any revised notice and consent framework.

5 For example, would using personal information for policy, evaluation, training surveys and other peripheral policy work fall within the concept of reasonable expectation?

6 See, for example, APP Guidelines, paragraphs [5.16], [6.25] and [6.27].

j. Enhanced clarity in respect of secondary purposes and 'reasonable expectation' would provide benefits to both agencies and the public by ensuring a greater capacity for agencies to share data relating to deceased individuals, reducing the risk of distress caused by correspondence being sent to a deceased individuals' next of kin.

8. Consent to collection and use and disclosure of personal information: Exceptions to the requirement to obtain consent

31. Are the current general permitted situations and general health situations appropriate and fit-for-purpose? Should any additional situations be included?

a. While the department acknowledges the flexibility offered by the seven exceptions set out in the permitted general situations under s 16A of the Act, the department is of the view that the flexibility provided by s 16A could be enhanced without compromising the scope of the protections set out in the APPs.

b. In particular, the department notes that s 16A, Item 1 is somewhat narrowly cast in terms of its ability to facilitate the disclosure of personal information in certain circumstances, most notably in the context of residential aged care facilities where the capacity to provide informed consent may be an issue.

c. For example, where an individual without the capacity to provide consent and without appropriate guardianship arrangements requires a health service and the non-provision of that health service may not necessarily result in a 'serious threat' to the individual's health, that individual may still be subject to adverse health outcomes as a result of not meeting the high threshold required under s 16A, Item 1 of the Privacy Act.

d. In the context of disclosures across jurisdictions, there are inconsistencies around when such disclosures can occur without consent, given the varying thresholds required to enliven analogous exceptions in state and territory legislative frameworks (where health providers are working under those frameworks, which is itself dependent on whether they are engaged by a private or public institution).

e. These inconsistencies may lead to a degree of uncertainty and have the effect of inhibiting the appropriate disclosure to at-risk individuals. Consistency across jurisdictions would provide greater clarity for health providers and the department would be supportive of appropriate measures to harmonise the relevant thresholds (see also discussion under Part 16 below).

f. Regarding s 16A, Item 2, the department notes that while the exception is intended to apply to an APP entity's internal investigations into unlawful activity or serious misconduct, the Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protections) Bill 2012* (at page 67) does not contemplate the exception applying to activities resulting in a breach of contract by contracted service providers.

g. The department would strongly support amendments to s 16A, Item 2 to ensure that the definition of 'unlawful activity' is extended to such actions that may lead to serious breaches of contract to provide agencies with the ability to undertake audits to ensure contracted service providers' compliance with relevant contractual provisions. The department would recommend limiting any such exception to serious breaches of contract where, for example, appropriate

expenditure of public funding is under threat or continuity of service for vulnerable clients may be at risk.

h. For example, in situations where the department identifies concerns that an in-home aged care service provider is not providing the services they have been funded to deliver (resulting in vulnerable senior Australians potentially being left without support), the ability to use or disclose information to confirm the extent of the failure and the magnitude of risk to members of the public would provide significant benefit to both the department and service recipients.

i. The addition of a specific exception to allow for the collection, use and disclosure of personal information in these circumstances, with appropriate restrictions (for example, reasonable belief there has been a serious breach of contract (including a potential serious breach), would provide agencies with an enhanced ability to ensure work undertaken by contracted service providers is undertaken appropriately and in line with relevant requirements and community expectations.

j. The department would also strongly support the definition of 'unlawful activity or serious misconduct' being expanded to include misuse of government funding in situations where it is unclear whether fraud may be occurring until further investigations are undertaken. The department does not consider that the above enhancements would have a detrimental impact on the protections afforded to individuals under the APPs.

9. Consent to collection and use and disclosure of personal information: Withdrawal of consent

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

a. The department is broadly supportive of any appropriate measures that would provide greater detail in relation to the currency of consent.

b. The Privacy Act provides no guidance as to the issue of currency of consent and while the APP Guidelines are helpful in further exploring the issue, a statutory test and an appropriate timeframe for determining currency may be beneficial in providing greater clarity for both individuals as well as the APP entities relying on those individuals' consent in the handling of personal information.

c. Further to a revised statutory framework for consent, the department notes it would be helpful for support materials to set out timeframes, a standard form of words and guidance to assist APP entities in meeting any new obligations regarding consent while at the same time managing information overload and consent fatigue.

10. Consent to collection and use and disclosure of personal information: Emergency declarations

41. Is an emergency declaration appropriately framed to facilitate the sharing of information in response to an emergency or disaster and protect the privacy of individuals?

a. The department broadly supports the emergency declaration powers available under Part VIA of the Privacy Act, however notes there is currently no ability to

selectively authorise particular collections, uses or disclosures of personal information under Part VIA.

b. In inter-agency discussions concerning the potential making of an emergency declaration under s 80J or s 80K in relation to the COVID-19 pandemic, there were concerns raised that there is no ability to selectively authorise specific information sharing acts or practices of particular types of entities.

c. Therefore, the department considers that greater flexibility in the application of the authorisations to share personal information, as determined by either the Minister or Prime Minister, would improve the balance between the need to protect the privacy of individuals and the need to share personal information to efficiently and effectively respond to emergency and disasters.

d. The effectiveness of Part VIA to facilitate sharing of personal information in response to emergencies or disasters is limited by s 80P(1)(d), which does not permit organisations to disclose personal information to a State or Territory authority. State and Territory authorities play a significant role in coordinating and responding to emergency and disaster situations under Australia's federal system. Therefore the department would welcome amendments to Part VIA to authorise organisations, which may hold personal information valuable in responding to emergency or disaster situations, to disclose personal information to State or Territory authorities for a permitted purpose.

e. In recognition of the rapid response required in emergencies or disasters of national significance and the associated resource constraints often faced by entities during these circumstances, the department queries whether the Information Commissioner's powers to direct agencies to give the Commissioner a privacy impact assessment (PIA) within a specified period under s 33D, should be modified when an emergency declaration is in force.

f. The department's acknowledges that a 'privacy by design' approach should be adopted even in emergencies or disasters and PIAs are an important and valuable tool to address privacy risks. However the department considers that the period specified by the Information Commissioner to undertake a PIA should, for the period during which the emergency declaration is in force, be required to take into account the timing and resource constraints often faced by agencies whose priority will be to assist individuals involved in the emergency or disaster.

11. Consent to collection and use and disclosure of personal information: Regulating use and disclosure

42. Should reforms be considered to restrict uses and disclosures of personal information? If so, how should any reforms be balanced to ensure that they do not have an undue impact on the legitimate uses of personal information by entities?

a. In line with the exception set out under APP 6.2(e), health information (including genomic information) may be disclosed for an 'enforcement related activity' under certain conditions.

b. The department notes that such disclosures are permitted for a wider range of offences than those for which primary genetic testing may be undertaken by law enforcement agencies at a state, territory and Commonwealth level, which is restricted to serious and indictable offences.

c. There is a risk that such broad permissions in the context of genomic information may undermine community confidence in the privacy of their genomic

information, which may in turn create a barrier to accessing services and participating in research.

d. The department would welcome any additional protections to enhance protections regulating the disclosure of genetic information for enforcement related activities to mirror the offences for which law enforcement agencies may undertake primary genetic testing.

12. Control and security of personal information: Security and retention

45. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

a. While the department supports any appropriate measures to ensure personal information is not unnecessarily retained by APP entities, any additional statutory requirements will need to be considered alongside existing retention obligations to which agencies are currently subject under the *Archives Act 1983* (**Archives Act**).

13. Control and security of personal information: Right to erasure

47. What considerations are necessary to achieve greater consumer control through a 'right to erasure' without negatively impacting other public interests?

a. The department is broadly supportive of the concept of providing individuals with a greater degree of control over their personal information, including an enhanced right to erasure set out in statute.

b. However, as with any changes to the obligations on APP entities to destroy or de-identify personal information, any such measures would need to take into account existing record management obligations to which agencies are subject under the Archives Act.

14. Overseas data flows and third party certification

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?
    a. Are APP 8 and section 16C still appropriately framed?

a. The department notes that there are presently a number of challenges arising under APP 8 which have become more pronounced with the increasing reliance on off-shore data storage through the use of third party cloud services providers.

b. APP entities such as the department are increasingly relying on engaging off-shore cloud services providers, for the purpose of providing the IT infrastructure to store the information being collected, used and disclosed by APP entities.

c. Further, as previously set out under the discussion regarding consent, the department notes the difficulties in obtaining consent to the exclusion of APP 8.1[7] can be problematic, particularly in the context of where personal information may be published online and accessible by individuals overseas. These additional

7 The exclusion of APP 8.1 refers to circumstances where 'an APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the APP entity expressly informs the individual that if they consent to the disclosure, this principle will not apply and the individual then consents to the disclosure' (see APP 8.2(b) and paragraph [8.27] of the APP guidelines).

obligations serve to complicate the notification process under APP 5 and may cause unnecessary confusion or alarm among individuals.

d. The department would welcome any alternative mechanisms that simplify this process and mitigate the risk of unnecessary confusion or alarm among individuals. Such mechanisms could be included in an enhanced consent framework (as previously discussed) and may involve the use of simplified or standardised wording or the increasing use of symbols or visual signposting.

15. Notifiable Data Breaches scheme: Impact and effectiveness

63. Have entities' practices, including data security practices, changed due to the commencement of the Notifiable Data Breaches Scheme?

a. Since the commencement of the Notifiable Data Breaches Scheme in February 2018, there have been a number of improvements across the department in relation to prevention practices, as well as identification and treatment of potential data breaches.

b. The department's data breach handling processes involve consideration, identification and recommendation of potential improvements to strengthen practices, processes and systems. There are a number of examples where, following investigation of incidents and the subsequent making of recommendations, a number of key business areas within the department have made significant enhancements to information handling practices and quality assurance processes to reduce the risks of inadvertent disclosures of personal information to incorrect recipients.

c. Additionally, as a result of the development and publication of the department's Data Breach Response Plan (the Plan), as well as the various privacy-focused communications and training activities undertaken in relation to the Plan, it is clear that there is a greater awareness and understanding across the department of the need to promptly report potential data breaches for investigation.

16. Interaction between the Act and other regulatory schemes

67. Is there a need for greater harmonisation of privacy protections under Commonwealth law?
    a. If so, is this need specific to certain types of personal information?

a. The department is broadly supportive of measures aimed at harmonising the privacy protections at the state or territory level with those at the Commonwealth level.

b. In particular, the department notes the potential benefits for both APP entities and individuals if there were greater consistency across jurisdictions in the definitions of key concepts including (but not necessarily limited to) 'personal information' and 'sensitive information'.

c. Further, greater consistency in terms of obligations to which APP entities are subject (that is, a degree of consistency with the APPs at the state or territory level) when handling personal information would simplify cross-jurisdictional work between the Commonwealth and state or territory entities.

d. For example, undertaking Privacy Impact Assessments or other comparable analyses of information flows involving the use and disclosure of personal

information between the Commonwealth and state or territory entities such as public or private hospitals, state health authorities would be significantly less complex and lengthy if all parties involved in the use and disclosure of that information were subject to a comparable set of obligations such as that set out in the APPs.

e. Further, the department notes current inconsistencies across jurisdictions in relation to the whether genomic information is also 'health information'. While under the Privacy Act genomic information is defined specifically as both sensitive and health information with more robust protections than other kinds of personal information, this is not consistent across state and territory regulatory schemes. This places a significant burden on health professionals who are required to be aware of, and comply with the different requirements based on whether they are working in public or private institutions and/or across state or territory borders.

f. Whether genomic information is defined as sensitive and health information has implications for the disclosure of this information under APP 6. Rules permitting disclosure to third parties operate with different thresholds and this may result in confusion and inhibit appropriate disclosure to at risk family members.

g. There are also inconsistencies across jurisdictions in relation to the protections afforded to the genetic information of deceased individuals, as well as a lack of clarity around how those protections regulate the disclosure of that information.

h. The department is broadly supportive of any appropriate measures aimed at harmonising the classification of genomic information as sensitive and health information across jurisdictions, as well as harmonising the conditions to permit disclosure of genomic information between jurisdictions and to at-risk relatives (including genomic information relating to deceased individuals).

i. In particular, the department notes inconsistencies between jurisdictions where it is unclear whether family members can request access to deceased persons' DNA for genomic sequencing for purposes relating to their health and/or family history and that this may be dependent on the jurisdiction the deceased person resides.

j. The department's view is that there should be a nationally consistency approach and note that further consultation is required regarding whether there needs to be updates to the Privacy Act or if this would most appropriately be addressed through other mechanisms (such as guidelines, FAQs or comparable support materials).