Submission to the Privacy Act Review Report

Thank you for the opportunity for Australian Genomics to provide a submission to the Privacy Act Review Report consultation.

About Australian Genomics

Australian Genomics is an Australian Government initiative supporting genomic research and its translation into clinical practice. Through broad engagement and a national collaborative approach, it achieves two key objectives: to improve efficiency, reach and timeliness of genomic research projects, and to support Commonwealth State and Territory health departments in the implementation of genomics research outcomes by refining and communicating evidence to inform policy development.

Australian Genomics engages with current and emerging government policy and priorities to identify gaps and opportunities, to support policy and action for integrating genomic technologies into the health system. By interfacing with consumers, governments, industry and global genomics initiatives, Australian Genomics drives change and growth in the sector.

Part 1: Scope and application of the Privacy Act

3. Objects of the Act

Section 3.3 general comments

Australian Genomics supports the Attorney-General's Department interpretation and summary of feedback received during the Privacy Act Report process, particularly in relation to the need to balance protection of privacy and other interests, and to give 'due weight to public interest activities, including research'. The identified need to modernise privacy legislation to promote digital trust is another important reason to review and progress amendments to the *Privacy Act 1988*.

4. Personal information, de-identification and sensitive information

Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.

The intent of this proposal is to broaden the definition of personal information to encompass related information when linked with specific external information. Whilst the context provided for this proposal is embedded in technical information, the broadening of the definition to use the word

'related to' rather than 'about' could have implications for collection, use and storage of familial data, which is often required for the interpretation of an individual's genomic test results.

In the context of genetics, genomics and some other types of health information collected about an individual when combined with other sources can make a related person identifiable. Changing the wording from 'about' the individual to 'related to' the individual could be interpreted as the APP entity holding personal information that links to a relative of the individual. However, the relative may not have a relationship with the organisation or agency that holds this data and has not consented to collection, use and storage.

Should the Proposal 4.1 be accepted, and wording of the definition changed from 'about' to 'related to', Australian Genomics would request that clarifications for managing familial data collection be addressed by provision of explanatory materials and OAIC guidelines.

Proposal 4.4 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment.

Australian Genomics supports the continued use of 'reasonably identifiable' rather than further defining reasonably identifiable as 'directly and indirectly identifiable' (as discussed in Section 4.3). The terms require clarification, such as by providing the suggested non-exhaustive list discussed in the Privacy Act Report, and by providing clarity about what would represent a situation where one could 'reasonably identify' an individual. It is preferable to keep the existing wording and instead work on clarification of the meaning and scope of the term.

The Privacy Act Report discusses that whether a person 'is reasonably identifiable will depend on the context in which the information exists, the means reasonably likely to be used to identify someone, from whose perspective the individual must be identifiable, and current data processing practices.' If Proposal 4.9 is progressed, both genetic and genomic information will be categorised as sensitive personal information, and the protections of the Privacy Act extended to it.

There has been discussion in recent years about whether genetic variant information is reasonably identifiable and thus covered by the Privacy Act. A genetic variant is an alteration in the DNA nucleotide sequence, which may be common in the population or rare. A single variant may be enough to cause a genetic condition, and variant information is often shared to international open access databases such as ClinVar (a public archive of human variants and related phenotype data owned by the NIH National Centre for Biotechnology Information). There is an increasing consensus that a genetic variant (however rare) is too small a unit of information to be reasonably identifiable. This has recently been discussed by Paltiel and co-authors who provide the arguments that no genetic variant is identifying without other information about the individual, and that variants are a

low privacy protection issue[1]. OAIC guidance should provide explicit advice on this issue to alleviate any remaining concerns.

Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context.

Contextualisation of de-identification within current environment and circumstances will work in many instances. It does for the most part appear to be a suitable compromise to the previously suggested proposal for de-identified data, given that most APP entities will remain active in data management. However, what happens if, in a future context, pseudo-anonymised data, anonymised data or data that is functionally anonymised in the public sphere becomes de-identified or reasonably identifiable data. It may not be possible to reassess data and recall data if context and circumstances change, resulting in a change of the data's position on the spectrum of identifiability. This proposal, or the resulting principles or advice, would need to address how **future rather than current** identifiability are managed within the scope of this change to the Act. This proposal potentially means that APP entities will need to process data using the most stringent de-identification practices for all personal information, in anticipation of an unknown, future context arising where it is potentially more reasonably identifiable.

Additional guidance would be welcome regarding what de-identification processes will be required for different types and combinations of personal data. We found the spectrum of personal information presented in the Privacy Act Report (pg 33, Diagram 1) a useful tool and would support its incorporation into supporting guidance from the OAIC and/or the APPs.

Proposal 4.9 Sensitive Information

(a) Amend the definition of sensitive information to include 'genomic' information.
(b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act.
(c) Clarify that sensitive information can be inferred from information which is not sensitive information.

Australian Genomics agrees that sub-proposal (a) genomic data should be considered on the same level as genetic data and that genomic data should be included in the Act, and that sub-proposal (b) and (c) should be applied to sensitive information to ensure consistency within the Act.

[1] Paltiel et al., (2023). International Data Privacy Law. ipad002

Part 2: Protections

10. Privacy policies and collection notices

Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.

Australian Genomics agrees with the implementation of industry specific standards. This should be done with community/consumer involvement and a co-design approach, and where collection notices are posted online, with user experience (UX) design input.

As part of collection notice standards, APP entities should be required to clearly communicate an individual's rights to access object, erasure, correction, de-indexing (Proposals 18.1 – 18.5), and that a nominal fee may be charged in the event an individual chooses to exercise these rights.

11. Consent and online privacy settings

Proposal 11.1 Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

In the Privacy Act Discussion Paper, the proposal was put forward to define consent to provide that it must be 'informed, voluntary, current and specific, and given with capacity' which has been slightly amended in the Privacy Act Report to 'voluntary, informed, current, specific and unambiguous through clear action'.

In our response to the Discussion Paper we raised concerns that the health and medical research sector needs assurances that information sharing for secondary purposes, including to future, unspecified research projects, will still be allowed given the 'specific' consent requirement. We reiterate those concerns here. While we agree that APP entities should not seek a broader consent than is necessary for its purposes, or for undefined future uses, large-scale health research initiatives (such as genomic research, biobanks and longitudinal studies) are set up with the intention to make the data they collect available to other research programs, that are *not specified at the time at which consent is obtained* from the individual. Given that for APP entities involved in research there are several pathways by which one can lawfully process data (consent being one of them), it would be good to have more specific guidance on the best practice lawful bases for different primary and secondary uses.

On the topic of currency of consent, the Privacy Act Report outlines 'OAIC guidance says that consent cannot be assumed to endure indefinitely, and it is good practice to inform individuals of the period that consent will be relied on'. However, HREC approvals for human research are often open-ended and consent would in most cases be considered current until formal closure of the project. This could represent an individual's lifetime for longitudinal, biobank or databank studies. Thus, more detailed advice about the 'current' requirement will be needed for entities doing health and medical research.

It should be noted that when GDPR introduced that consent should be 'freely given, specific, informed, and unambiguous' it was accompanied by an expectation that other lawful bases for data processing would be relied upon more frequently, such as legitimate interest or public interest[2]. This is because for any consent process to achieve the rigorous expectations of GDPR would be difficult. Therefore, how entities working under the Australian Privacy Act that are involved in data processing/secondary use can achieve consent of this nature is unclear. One alleviating mechanism will be having one set of rules for agencies and organisations (Proposal 14.3) so that organisations can also progress research in the public interest if obtaining consent from the individual is impractical. Dynamic consent has been proposed as one mechanism that could fulfil the requirements for data processing through consent of the individual under GDPR[2].

The Privacy Act Report mentions that consent fatigue can result from being overwhelmed with the number of consents an individual is required to give, and thus causes disengagement from consent. There are emerging technologies and digital trust solutions being developed that facilitate individuals to self-manage consent settings across their digital interactions rather than providing individual consent for each interaction. These technologies should be further explored to limit consent fatigue. Although consent fatigue is referred to frequently in the health and medical bioethics and ELSI literature, we have found it difficult to find any empirical research demonstrating that consent fatigue is a genuine issue in this sector.

The Privacy Act Report seems in favour of placing less emphasis on consent from the individual but instead rely more on introducing proposals to strengthen the individual's rights in the event they become unsatisfied with the processing of their personal information (e.g. right to explanation, to object, to opt-out, erasure – Proposal 18.1). It could be argued that providing proper mechanisms to give consent upfront would be less burdensome and complicated than an individual trying to exercise their rights in the event they identify unfair or unreasonable sharing of their personal information has occurred.

12. Fair and reasonable test

[2] Prictor et al., (2019). Journal of Data Protection & Privacy. Vol.3, 1 93–112

Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

Applying a fair and reasonable test would enable principles used to inform these concepts to be adjusted to the environment and context overtime. This would enable flexibility and adaptability in the Act.

Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

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

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include:

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

The fair and reasonable test (f) outlines that collection, use and disclosure of personal information must be in the best interests of *the* child. Sometimes, personal information is processed for health and medical research where the primary benefit will be for *all* children, rather than *the* child. Therefore, will guidance clarify whether research in the public interest will satisfy this fair and reasonable test for the processing of children's personal information? Otherwise, this proposal may result in significant restrictions to health medical research.

Australian Genomics also offers the suggestion that if children are singled out as having different considerations in the fair and reasonable test, should the Proposal 12.2 also consider whether the

collection, use and disclosure of the personal information of *all vulnerable people, and minority groups*, is fair and reasonable.

Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed.

Australian Genomics agrees with this proposal. In the context of APP's listed and the rationale presented, this proposal should not impact research data or clinical data collection, use and disclosure.

13. Additional protections

Section 13.4 general comments

The Privacy Act Discussion Paper Proposal 10.4 sought to 'Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose' and asked, 'Would the proposed definition of a secondary purpose inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research?'.

The Privacy Act Report outlines that submitters to the Discussion Paper were equally concerned about the proposal resulting in narrowing and broadening the scope of a secondary purpose. These opposing interpretations showed that the proposal was not fit for purpose and contributed to no proposal being put forward for further consideration.

Defining a secondary purpose as having to be 'directly related to' and 'support' the primary purpose would be very limiting for the purposes of health and medical research. Not providing a definition for 'secondary purpose' maintains the status quo and does not introduce further restrictiveness to public interest uses.

Proposal 13.1 APP entities must conduct a privacy impact assessment for all activities with high privacy risks.

- **A privacy impact assessment should be undertaken prior to the commencement of the high-risk activity.**
- **An entity should be required to produce a privacy impact assessment to the OAIC on request.**
- **The Privacy Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals.' OAIC guidance should be developed which articulates factors that that may indicate a high privacy risk, and provides**

examples of activities that will generally require a privacy impact assessment to be completed. Specific high-risk practices could also be set out in the Act.

In section 14.1 of the Privacy Act Report, the role of HREC in assessing public interest in privacy is discussed, with mixed perspectives from respondents. When we consider PIAs for researcher activities, these assessments would be a useful information source for HREC when reviewing privacy in the context of public interest. It would be reasonable to include PIAs as part of the ethics submission to HREC. However, HREC would need support in incorporating this type of documentation into review processes. It would be our recommendation that for any changes related to research (Section 14, Proposals 14.1 to 14.3) there be guidelines by OAIC, in partnership with NHMRC, that define roles and responsibilities of HREC in privacy decision-making, particularly if PIAs are being supplied to HRECs as part of project documentation.

Proposal 13.4 Include an additional requirement in APP 3.6 to the effect 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. OAIC guidelines could provide examples of reasonable steps that could be taken.

OAIC guidelines would be helpful to determine when an entity can collect information relating to an individual but not directly from the individual. OAIC guidelines should include HREC review and consent by the individual as mechanisms for proving data was collected by lawful means.

14. Research

Proposal 14.1 Broad consent for research
Introduce a legislative provision that permits *broad consent* for the purposes of research:

(a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply.

(b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained.

Sub-proposal (b): How will a 'research area' be defined - will there be guidance from the OAIC or will it be left up to individual organisations to define and satisfy themselves that research areas are not overly broad?

Demonstrating the various interpretations of research areas permitted for secondary research through broad consent models, below are examples of different broad consent clauses applied to genomic research consent for secondary research use of data:

- Secondary research use must be related to the condition of the individual (e.g. cardiovascular genetic disorders)

- Secondary research can include all ethically approved research
- Secondary use for categories defined by the Global Alliance for Genomics and Health's Data Use Ontology standard outlines 'general research use'; 'health, medical and biomedical research'; 'population and ancestry research'.

As outlined in the Privacy Act Report, GDPR states that: 'Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose' and that where granular consent options are possible individuals should be able to consent to parts of research projects. As a result of the GDPR's wording of the broad consent clause and difficulties of interpreting this clause, the 'public interest' mechanism is primarily used by researchers to enable secondary use in GDPR/Europe. It is Australian Genomics' view that while broad consent is convenient and acceptable to most individuals participating in health and medical research, more granular and dynamic consent options should be available to those who want more control over the use of their personal information. However, care must be taken in wording of the broad consent clause in the Privacy Act and associated guidance to ensure that it is practical to implement.

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

Currently, the exceptions for agencies are for health and medical research only, but apply to all personal information and offer derogation from the APPs. In contrast, exceptions for organisations apply to a broader scope of research, but only to health information. Development of a single set of guidelines for research conducted by organisations and agencies would provide clarity about permitted purposes, and as outlined in the Privacy Act Report, facilitate entities involved in research to navigate the collection, use, and disclosure of personal information utilising the consent exception more confidently. A single set of guidelines would make collaborative research between agencies and organisations easier to navigate and improve ability for public interest research by agencies and organisation that request agency data.

From the perspective of consent, organisations and agencies would be able to rely on doing research in the public interest without consent (though would still need to get HREC approval and demonstrate the impracticality of obtaining consent). This would likely serve to increase the scope and pace of important research. As an organisation involved in research, we are very familiar with the conservative approach to interpreting the guidelines, including determining when consent of the individual is not required under the medical research exception.

18. Rights of the individual

Erasure

Proposal 18.3 Introduce a right to erasure with the following features:

(a) An individual may seek to exercise the right to erasure for any of their personal information.
(b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

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

Australian Genomics seeks clarification on the level of erasure required, as research entities will need to have exemptions such as to hold data until retention periods have elapsed. When a participant withdraws from a research study this is not the same as requesting erasure. If erasure becomes an option under the Privacy Act research may need to be exempt due to the NHMRC requirement to archive data (15 years for clinical trials, 5-10 years for other types of research). Even if the data is not used, data retention maybe critical to future legal challenges or serious adverse event investigations, for example if a participant is given a drug in a clinical trial, it is unreasonable to erase that data if they choose to withdraw from the study.

Proposal 18.8 An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act.

This proposal is acceptable as long as the word 'reasonable' is maintained. In the example of genomic data, it would be unreasonable for an APP entity to provide technical support to enable an individual to understand their raw genomic data or access or store their data on an appropriately supported platform (i.e. cloud), but it would be within scope to provide FAQ sheets on managing genomic data that is supplied to them.

23. Overseas data flows

Proposal 23.1 Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.

It is unclear from the proposal if the 'Australian link' applies to research entities when sharing for secondary purposes if it is not specifically mentioned in the research exemptions. This is something to consider in the consultation process. For example, de-identified datasets are shared to international repositories as part of academic journal publication requirements, but there is no other link for that data between Australia and the country where the repository is maintained.

All objects of the revised Privacy Act should be designed in a way to ensure they enable the principles of Indigenous data sovereignty.

Part 3: Regulation and enforcement

28. Notifiable data breaches scheme

Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.

Proposal 28.2

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

The proposal imposing a 72-hour time limit for notification to the OAIC of a potential eligible data breach, rather than 'as soon as practical', is maintained despite opposition by some submitters to the Discussion Paper. Implementation of this proposal will raise certain issues, including whether the business operates 24/7 and thus can report within the required timeframe, or whether enough information can be gained about the issue in the timeframe. This timeframe may create administrative burden to OAIC due to reporting of events that are later found not to be data breaches but are reported due to the time limit.