napwha national association of people with HIV australia

Australian Sex Workers Association

Department of Prime Minister and Cabinet
Office of the National Data Commissioner
PO Box 6500
Canberra ACT 2600

6th November 2020

Re: Data Availability and Transparency Bill 2020 Exposure Draft Consultation Paper

To the Office of the National Data Commissioner,

Thank you for the opportunity to provide feedback on the *Data Availability and Transparency Bill 2020* Exposure Draft Consultation Paper.

The National Association of People

with HIV Australia (NAPWHA) is the peak non-government organisation representing community-based groups of PLHIV across Australia. We provide advocacy, policy, health promotion, effective representation, and outreach on a national level. Our work includes a range of health and education initiatives that promote the highest quality standard of care for HIV-positive people. Our vision is a world where all people with HIV can reach their full potential free from stigma and discrimination.

Scarlet Alliance, Australian Sex Workers' Association is the national peak sex worker organisation in Australia. Formed in 1989, the organisation represents a membership of individual sex workers and sex worker organisations, projects and collectives throughout Australia. Scarlet Alliance and our member organisations and projects have the highest level of contact with sex workers in Australia of any agency, government or non-government. Through our project work and the work of our membership we have consistently maintained high levels of access to sex industry workplaces in the major cities and many regional areas of Australia.

Background

NAPWHA and Scarlet Alliance have had the opportunity to review the joint submission made by NAPWHA's member organisation Positive Life NSW and the HIV/AIDS Legal Centre. We support the comments and conclusions reached in that paper. We would also like to take the opportunity to supply the following additional comments on the exposure draft.

Simplified outline

It is of concern that the simplified outline of the Bill in s.4 attributes to the National Data Commissioner, as the regulator for the data sharing scheme, the function of advocating only for the greater sharing and release of public sector data. This ignores the reality that, in many circumstances, data is sensitive and sharing and release should be advocated *against*; such as where the risk of harm outweighs benefit to the person whose data is being shared. Ever greater sharing of information is not self evidently beneficial and the section should not assume as much.

The Commissioner's role should be, first and foremost, to protect the privacy and safety of individuals against threats of unnecessary or unauthorised sharing of their data. Only where

privacy has been safeguarded and where perilous sharing of data has been prevented, should the Commissioner be tasked with promoting broader sharing of information.

We recommend that the simplified outline of s.4 should articulate the Commissioner's role as being to protect the privacy of individuals whose data is being shared and to strike a balance between the threats and benefits of data sharing.

Data Sovereignty and Consent

NAPWHA and Scarlet Alliance maintain that individuals should remain sovereign over their own data. Data about an individual should remain the property of that individual at all times. Individuals should be able to gain free access to data held about them and to alter, delete and correct their data where there are inaccuracies. Individuals should be able to provide their data, and withdraw it, at any time from any provider of data services. Individuals should be free to sell their data or provide it in exchange for services and there should be consumer choice as to the provider of data services. Where data entities misuse data, individuals should be free and entitled to remove their data from that provider and place it with a provider they have confidence in.

It is of concern to NAPWHA and Scarlet Alliance that the Bill treats data as if it is not the property of the individual. Under this proposed legislation individual sovereignty over one's own data is limited to the ability to give or withhold consent to its sharing as per the data sharing principles in s.16. Further, this consent is articulated as a mere principle under s.16 of the Bill and not as a mandatory pre-requisite of data sharing.

We also note that the language used in s.16 is such as to allow data collection without consent where obtaining consent would be 'unreasonable or impractical'. This would likely permit the sharing of an individual's data where that data is part of a mass, deidentified data set even where that individual had refused or withdrawn consent to its sharing. In extreme cases this may even allow sharing of data in cases where individuals have expressly refused their consent, thus rendering obtaining consent 'impractical'. A further concern is that data sharing entities will insert blanket consent provisions into their terms of service that will undermine any meaningful ability of individuals to give informed consent to the sharing of their data. Thus, the Bill fails to provide adequate motivation for data sharing entities to obtain consent and similarly, it fails to provide adequate redress where sharing contrary to the wishes of individuals occurs.

We recommend that the principle of individual data sovereignty described above be clearly articulated in the simplified outline of Chapter 2 at s.12. We further recommend that it is inserted into the data sharing principles in s.16 and that this principal is clearly identified as taking precedence over all other principals and data scheme stakeholders.

We strongly recommend that s.17 be amended to include a sub-section which excludes data from the sharing scheme where an individual has not given consent, has expressly refused their consent or has withdrawn their consent to the sharing of their data. Further, the sub-section should articulate that individuals can give, refuse or withdraw consent by communicating this verbally or in writing to a data custodian or a data scheme entity.

We recommend that where sharing occurs without consent a redress and financial compensation mechanism for the individual whose data has been shared contrary to their wishes should be included in the Bill at Part 5.5. Financial compensation should be proportionate to the severity of the negative consequences caused by the unauthorised sharing of data. Data shared in an unauthorised way must be required to be destroyed and permanently deleted from all databases.

Prohibition on taxpayer exploitation

Data collected by Commonwealth agencies using taxpayer's money should not be allowed to be shared for research and development (s.8(c)) to create products which will then be privately sold back to individuals or governments. This would amount to a socialising of the costs of private industry but a privatisation of its benefits.

The products of research and development using taxpayer's data must remain in the public domain and be available for the free use by, and benefit of, Australian Citizens and residents that have, at significant cost, funded the collection of their own data on their behalf through their taxes.

If public money is used to collect data which, in turn, is used to extract further profit from the citizens whose taxes have paid for the establishment of the proposed system, then public confidence in the system, trust in the government and consent to data collection, sharing and storage will be significantly undermined.

The products of all research and development using Australians' data must therefore be 'open source' and remain in the public domain. This does not preclude the making of profit. However, the intellectual property rights of all data and all outputs derived from that data must remain in the public domain.

We recommend that the products of all research and development using Australians' data (and the data itself) must remain in the public domain. Accordingly, the output principle in s.16(5) should be amended to include an additional provision that 'no data or output can be privatised for profit or otherwise. All outputs must remain publicly accessible and in the public domain'. Sections 13 and 14 must be amended to preclude sharing otherwise than in accordance with the revised outputs principle.

Enforcement purposes

Section 15(2) and (3) of the Bill preclude the sharing of data for enforcement purposes. We welcome these provisions. However, they do not go far enough and are immediately negated by s.15(4).

Data cannot be shared under 15(2) and (3) if it directly relates to an enforcement purpose. However, s.15(4) allows sharing of data, including for enforcement related purposes, in situations where it is 'generally relating' to an enforcement purpose. This negation of the protections contained in s.15(2) and (3) is cynical and does little to encourage trust in the system proposed by the Exposure Draft.

Under the current s.15 of the Bill data could be shared for 'research and development' into enforcement related technologies, for example. The Bill would not prevent a situation similar to

that in the USA where facial recognition software, built using citizens' photo data on Facebook is now being used by police forces to surveil and police the very citizens whose data made the technology possible[1].

We also note that the communities that NAPWHA and Scarlet Alliance represent have long histories of harassment, surveillance and over-policing by the state. Hostile policing and discriminatory treatment still prevail both at an individual and at the community level. For members of these communities to confidently engage with government services, such as health services, significant levels of trust are required. Distrust, caused for example by the government allowing citizens' data to be used against them for enforcement purposes, has the potential to drive members of vulnerable communities away from the services they require. As we have recently experienced in relation to COVID-19, when this happens, it has serious negative impacts on the public health response in Australia and this affects all of us.

We strongly recommend that the government build trust with vulnerable and marginalised communities by prohibiting the sharing of data for all reasons related to enforcement purposes no matter how indirect. Accordingly, we strongly recommend that s.15(4) be removed in its entirety.

Sharing data overseas

This Bill relates to Australian citizens and residents engaging with Australian websites on Australian servers to access, modify and create sensitive personal data such as tax, social security, MyGov and MyHealthRecord information. It is therefore extremely alarming that the Bill contemplates, under section 8(d), the sharing of data with 'foreign persons' in accordance with 'international agreements'.

All data shared under this Bill or any other Australian Act should remain in Australia at all times. Overseas entities are not subject to the same rigorous Australian data security and privacy standards. Continued Australian oversight of overseas entities is impossible. In the event of harm occasioned by data mismanagement, international agreements generally provide only limited recourse for governments and occasionally for multi-jurisdictional corporations but rarely for individuals.

The origin and history of the development of the internet is such that any data which travels overseas almost always travels through the internet infrastructure of the United States of America. This is because the internet originated in America as a military application. Any data that goes through the USA is subject to the *Patriot Act* and other American surveillance legislation that is significantly more invasive than that which Australians have to date accepted. This means that when Australians' data is shared overseas, it can be used by the US government to undertake surveillance of Australians that far exceeds Australians' expectations of an acceptable incursion into their privacy.

Data shared with overseas entities in this way can be used by governments and other entities to go around Australia's domestic privacy protections. For example the Australian government can avoid breaching its own privacy laws by making agreements with overseas entities to spy on Australian citizens. This undermines all of the protections and principles contained in the

[1] https://www.usatoday.com/story/tech/2020/07/23/facebook-offers-650-million-settle-facial-recognition-class-action/5498792002/

Exposure Draft. Allowing data to be shared with an entity in a jurisdiction which has poor regulation of data sharing arrangements also carries significant risk of security and data breaches.

In this way data can easily be shared for enforcement purposes, for surveillance, for profit extraction and for purposes that breach privacy and human rights protections. Data breaches can be covered up or remain undiscovered so that the harm they cause cannot be mitigated. The practical impossibility of maintaining oversight of foreign entities undermines the Australian Government's ability to protect Australians from the negative consequences of overseas data breaches. In turn this will damage trust in government and in the data sharing system proposed by the Bill.

We recommend that section 8(d) be deleted in its entirety and that an additional s.9 is added to Chapter 1 which expressly precludes the sharing of any data subject to this Act with any overseas entity or foreign person, regardless of international agreements.

Data Breach, Transparency, Complaints and Compensation

Part 3.3 of the Bill defines what is meant by a 'data breach' and provides that in the event of a data breach (or a suspected data breach) a data scheme entity must take reasonable steps to prevent or reduce any harm resulting from the breach to 'entities or groups of entities'. Here 'entities' as defined in section 9 includes individuals. The principle of minimising and mitigating harms to individuals attendant on data breaches is a sound one. However, the Part does not go far enough in terms of transparency or redress for individuals harmed by a data breach.

We strongly recommend;

1) That Part 3.3 be amended to require all data scheme entities to notify the Commissioner of any actual or suspected data breach regardless of seriousness, potential harm or whether the disclosure is required under the Privacy Act 1988 or the Data availability and Transparency Bill 2020 when it becomes law. All data breaches are opportunities to improve data management procedures. It is short-sighted to require notification to the Commissioner only in cases where data breaches can reasonably be concluded to be likely to result in serious harm as in s.37. All data breaches should be notified to the Commissioner then recorded, documented and investigated for their potential to improve the data sharing system in future. Further, the Commissioner must be required by that section to make a mandatory public disclosure in the event of a data breach to ensure transparency and public accountability.

2) That the complaints mechanism in part 5.3 be expanded to enable individuals whose data is being held by a data scheme entity (or entities) to complain to the Commissioner if the complainant reasonably believes a data scheme entity has breached its obligations under the Act, that there has been a data breach, or that the complainant's data has been accessed or shared contrary to the Bill or the Privacy Act 1988. Currently this section only applies to 'data scheme entities' and not to individuals whose data is being held. The interest of all Australians whose data is being held by data scheme entities cannot be appropriately safeguarded, or harnessed to improve the system and its security in future, if Australian citizens and residents are effectively excluded from making complaints in the event of data mismanagement. Further, the omission of a complaints mechanisms for individuals effectively shields data scheme entities

from public criticism of poor data management. This cannot encourage optimal data security and is a significant flaw in the proposed system of data sharing.

3) In the event of any data breach and particularly in the event of a data breach that results in harm, such as unwanted disclosures of HIV status, trans experience, sex work or other personal information, individuals must have the ability to bring an action for compensation against the entity that is responsible. We firmly believe that the best incentive for appropriately careful and diligent data management is liability to the individuals harmed by data mismanagement. Liability to individuals harmed in this way should exist in addition to the penalty provisions in section 99-102 of the Bill. Conversely, shielding data scheme entities from responsibility for poor data breaches will allow such entities to act with impunity. This will encourage sub-optimal data management practices and it will undermine public trust in the system.

Additional Comments

The Bill is unsatisfactory in several respects relating to the lack of a complaints mechanism for individuals concerned about misuse of their data. If such a mechanism exists by way of a complaint to the Office of the Australian Information Commissioner then this Bill should clearly specify this procedure. However, we note that such a complaint mechanism, if it exists, would first require individuals to complain to the agency responsible for the suspected data mismanagement. It is unclear how individuals can discover if their data has been mismanaged in order to make such a complaint. This is a serious flaw with this draft.

We recommend that the Bill specify that individuals concerned about data mismanagement can make a Freedom of Information Request to the data entity suspected. Further, as this Bill will create the position of National Data Commissioner in s.40, then it would be appropriate to build a complaints mechanism for individuals into this Bill to that Commissioner.

We recommend that in addition to the decisions of the National Data Commissioner, the decisions of data scheme entities should also be subject to merits review in the Australian Administrative Appeals Tribunal. Data scheme entities are, by virtue of their possession of either government data (or other data) to be used in the delivery of government services, agents or representatives of the government. The Bill should, therefore, specify that their decisions are subject to review. This would in part remedy the lack of accountability evident in this Bill.

Further to this point on transparency and accountability, we recommend that the annual report required to be prepared by the Commissioner under s.124, and given to the Minister for presentation to the Parliament, should contain detailed quantitative and qualitative information on the number and nature of data breaches, complaints that have occurred, and remedial action undertaken, in the past year to prevent future breaches. It should be made publicly available.

Recommendations

1) *We recommend that the simplified outline of s.4 should articulate the Commissioner's role as being to protect the privacy of individuals whose data is being shared and to strike a balance between the threats and benefits of data sharing.*

2) *We recommend that the principle of individual data sovereignty be clearly articulated in the simplified outline of Chapter 2 at s.12. We further recommend that it is inserted into the data*

sharing principles in s.16 and that this principal is clearly identified as taking precedence over all other principles and data scheme stakeholders.

3) *We strongly recommend that s.17 be amended to include a sub-section which excludes data from the sharing scheme where an individual has not given consent, has expressly refused their consent or has withdrawn their consent to the sharing of their data. Further, the sub-section should articulate that individuals can give, refuse or withdraw consent by communicating this verbally or in writing to a data custodian or a data scheme entity.*

4) *We recommend that where sharing occurs without consent a redress and financial compensation mechanism for the individual whose data has been shared contrary to their wishes should be included in the Bill at Part 5.5. Financial compensation should be proportionate to the severity of the negative consequences caused by the unauthorised sharing of data. Data shared in an unauthorised way must be required to be destroyed and permanently deleted from all databases.*

5) *We recommend that the products of all research and development using Australians' data must be 'open source' and remain in the public domain. Accordingly, the output principle in s.16(5) should be amended to include an additional provision that 'no data or output can be privatised for profit or otherwise. All outputs must remain publicly accessible and in the public domain'. Sections 13 and 14 must be amended to preclude sharing otherwise than in accordance with the revised outputs principle.*

6) *We strongly recommend that the government build trust with vulnerable and marginalised communities by prohibiting the sharing of data for all reasons related to enforcement purposes no matter how indirect. Accordingly, we recommend that s.15(4) be removed in its entirety.*

7) *We recommend that section 8(d) be deleted in its entirety and that an additional s.9 is added to Chapter 1 which expressly precludes the sharing of any data subject to this Bill with any overseas entity or foreign person, regardless of international agreements.*

8) *We recommend that Part 3.3 be amended to require all data scheme entities to notify the Commissioner of any actual or suspected data breach regardless of seriousness, potential harm or whether the disclosure is required under the Privacy Act 1988 or the Data availability and Transparency Bill 2020 when it becomes law. All data breaches are opportunities to improve data management procedures and should be investigated for their potential to improve the data sharing system in future. The Commissioner must be required to make a mandatory public disclosure in the event of a data breach to ensure transparency and public accountability.*

9) *We recommend that the complaints mechanism in part 5.3 be expanded to enable individuals whose data is being held by a data scheme entity (or entities) to complain to the Commissioner if the complainant reasonably believes a data scheme entity has breached its obligations under the Act, that there has been a data breach, or that the complainant's data has been accessed or shared contrary to the Bill or the Privacy Act 1988.*

10) *We recommend that, in the event of any data breach and particularly in the event of a data breach that results in harm such as unwanted disclosures of HIV status, trans experience, sex work or other personal information, individuals must have the ability to bring an action for compensation against the entity that is responsible. This should be added to the penalty provisions in section 99-102 of the Bill.*

11) *We recommend that the Bill specify that individuals concerned about data mismanagement can make a Freedom of Information Request to the data entity suspected. Further, as this Bill will create the position of National Data Commissioner in s.40, then it would be appropriate to build a complaints mechanism for individuals into this Bill to that Commissioner.*

12) *We recommend that the annual report required to be prepared by the Commissioner under s.124, and given to the Minister for presentation to the Parliament, should contain detailed quantitative and qualitative information on the number and nature of data breaches, complaints that have occurred, and remedial action undertaken, in the past year to prevent future breaches. It should be made publicly available.*

Aaron Cogle

Executive Director

National Association of People with HIV

Jules Kim

Chief Executive Officer

Scarlet Alliance