Summary of the Privacy Impact Assessment of the Data Exchange

Introduction

The Data Exchange was introduced by the Department of Social Services (the Department) in July 2014 as a new approach to collecting and using program performance data in order to reduce red tape for service providers and shift the focus of performance measurement from 'outputs' to more meaningful information about service delivery 'outcomes'.

Underpinning this approach is the reporting of client level information in the form of unit records. 'Client level data' refers to data collected and reported on each individual client rather than as summary (aggregate) data, such as counts of people that attended a particular program.

While some programs in-scope for the Data Exchange had reported client level data for many years, there are other programs for which this approach was new. This summary document is intended to help service providers and stakeholders understand how the Department considers privacy as part of the Data Exchange, and to provide context for how service providers may deal with their own privacy obligations.

Protecting client privacy, consistent with the Department's obligations under the *Privacy Act 1988* (Privacy Act), is a fundamental design principle of the Data Exchange and has informed the Department's operation of the Data Exchange since it was introduced.

As a routine part of assessing the privacy impacts arising from the operation of the Data Exchange, in 2015 the Department commissioned the Australian Government Solicitor to undertake a privacy impact assessment (PIA). More information about what a privacy impact assessment is and when they should be conducted is available on the website for the Office of the Australian Information Commissioner.

The PIA assessed the Department's operation of the Data Exchange, looking at the Department's obligations under the Privacy Act and making seven recommendations (available on pages 3 to 4 of this document). The recommendations and other key findings of the PIA, and the Department's response are outlined below. The PIA as a whole document can also be viewed, should readers require an additional level of technical detail. This information is being released in the interests of transparency and accountability, and to provide assurance to service providers and other stakeholders about the privacy protections in place to support the Data Exchange.

Summary of PIA recommendations

The PIA made seven recommendations to enhance the Department's arrangements for protecting the privacy of personal information while operating the Data Exchange. The recommendations primarily related to strengthening the processes already put in place, and where action was required in response to a recommendation, such as updating the Department's privacy policy (recommendation 1) , this was quickly acted on. No technical changes have been made or were necessary to the practical operation of the Data Exchange IT system in response to the recommendations.

The findings of the PIA identified some important privacy protections that were operating well, including the design of key privacy controls already incorporated in the design of the Data Exchange.

In response to **recommendation 1**, the Department's Privacy Policy was updated to reflect the operation of the Data Exchange. The Privacy Policy, available at https://www.dss.gov.au/privacy-policy provides information about the Department's general obligations under the Privacy Act and outlines the process for how individuals can make a complaint, access their personal information, or provide feedback.

Recommendation 2 related to the internal arrangements for Departmental staff working in the area where the client level unit records are stored, to ensure that they are aware of the legislative arrangements governing the data and also ensure that training and regular reviews are conducted. Although this was already happening, the Department formalised the processes in which it happened in response to this recommendation.

The PIA **recommendations 3**, **5** and **6** related to collecting and storing personal information in the Data Exchange, within the client management functions of the web-based portal available to service providers. The PIA suggested that the Department enhance the consent and notification arrangements in the Data Exchange Protocols so that:

- It is clear to clients that the Department is making the Data Exchange web-based portal available to service providers for providers' own client management purposes; and
- It is clear that service providers using the Data Exchange web-based portal for their own client management purposes are required to seek their client's express consent, on the Department's behalf, for the Department to store the client's personal information for these purposes.

These recommendations were addressed through the release of the October 2015 version of the Data Exchange Protocols and are identified in the version control history in Attachment 2 of the document. A 'client privacy brochure' was also released in December 2015 to help clients understand the arrangements that the Department has put in place to protect their personal information.

Recommendation 4 related to the Department's arrangements with service providers for follow-up client surveys. As a result, those arrangements no longer require providers to store a client's personal information where the client wishes to participate in these surveys. This change was formalised through amendments made to the October 2015 version of the Data Exchange Protocols.

In addressing **recommendation 7**, the Data Exchange self-service reports are built in line with the PIA recommendations and a future chapter of the PIA will be conducted as the Partnership Approach reports are progressing. This future work will take account of the recommendations and advice already provided in the current PIA and any new legislative and/or community expectations at the time.

Departmental response

The Department welcomes the recommendations of the PIA of the Data Exchange and the opportunity they provide to enhance the Department's arrangements for protecting personal information. The Department recognises that maintaining good privacy practices is a process of continuous improvement, and is committed to continuing its assessment of the possible privacy impacts of its operation of the Data Exchange. This includes ensuring that any future changes or additions to the Data Exchange continue to be designed and built with effective privacy protections in place.

Future chapters of the PIA are expected, as new functionality of the Data Exchange is progressed, such as the Partnership Approach reports. Documenting a PIA takes place with the functionality, design and build process, so that an assessment can be made within the operational workflow, rather than attempting to assess how things are expected to work. Any new chapters to this PIA will be released in line with transparency and accountability principles for the release of this document and to demonstrate the level of assurance of the privacy protections in place for the Data Exchange.

#	Recommendation	Implementation
1	Review and update the Department's general Australian Privacy Principles (APP) privacy policy now, and update that policy as necessary, to ensure that it reflects the Department's practices for managing personal information in relation to its operation of the Data Exchange. Additionally, regularly review that policy, and update it as necessary, to ensure that it reflects any changes to the Department's specific information handling practices relating to the Data Exchange.	In addition to reviewing and updating the Department's general APP privacy policy in line with the PIA, the Data Exchange team is consulted in processes for making major updates to the policy. The Department's privacy policy is available at https://www.dss.gov.au/privacy-policy
2	Take appropriate steps to ensure that, when accessing the database in which client-level unit records are stored, database administrators understand why they need to comply with relevant Departmental privacy and security procedures, and how they are to comply with these procedures.	The Department incorporated processes into departmental policy that specifically address the relevant departmental privacy and security procedures for accessing the database in which client-level unit records are stored, consistent with the Australian Government Protective Security Manual. Training is administered as a routine part of the implementation of these policies.
3	To eliminate the risk that the Department is presently operating the Data Exchange in a way that does not comply with APPs 3.1 and 3.3, decide, as a matter of priority, whether the client management system functionality of the Data Exchange will be made available to service providers who undertake program reporting by way of system to system transfers or bulk uploads.	The Department decided that the client management functionality of the Data Exchange will be made available to service providers who report by way of a system to system transfer or bulk upload. This decision was implemented by revising the scope of the consent and notification arrangements (as set out in the 'Protecting Client's Personal Information' section of the Data Exchange Protocols document) so that they apply equally to providers reporting through the web-based portal, system to system transfer or bulk upload, and to those service providers who intend to use the Data Exchange for client management purposes. (See also the responses to recommendations 5 and 6).
4	Confirm the need for service providers to store client contact details to facilitate follow-up client surveys.	The Department decided that there is no need for service providers to store client contact details to facilitate follow-up client surveys. Consequently, the Department no longer requires service providers to retain client contact details for this research. This decision to simplify requirements was implemented by the amendment of the Data Exchange Protocols document in the 'Protecting Client's Personal Information' section, in order to remove the requirement for providers to store client contact details separately from the Data Exchange for the purposes of facilitating follow-up client surveys.

#	Recommendation	Implementation
5	Enhance present arrangements with service providers using the web-based portal as a client management system to ensure that the Department is fully complying with APPs 3.3(a)(i) and 3.6 in collecting a client's personal information from those service providers.	In addition to extending the scope of the current arrangements for obtaining client consent (as required under the 'Protecting Client's Privacy' section of the Data Exchange Protocols) so that they also apply to providers who report via system to system transfer or bulk upload, and to those who intend to use the client management functionality of the Data Exchange, these arrangements have been further strengthened to ensure that the Department is collecting a client's personal information from service providers with the client's consent in the following ways by: o amending the above section of the Data Exchange Protocols to require providers to obtain, on the Department's behalf, the express consent of a client, noting there is a reasonable prospect that sensitive information (i.e. CALD, Indigenous and disability status) will be collected; o including procedures or systems for the recording of the client's consent by the service provider when reporting to the Department for all transmission methods; o introducing dedicated arrangements to address particular issues that arise with respect to the capacity of particular individuals to consent, including updating the Data Exchange Protocols to appropriately underpin these arrangements; and o amending the above section of the Data Exchange Protocols to require the provider to inform the client that they may withdraw their consent at any time, and include procedures or systems for the recording by the service provider of a client's decision to withdraw their consent and the processing by the Department of that decision.
6	Revise the 'DSS standard notification' to ensure that the Department is appropriately complying with APP 5 in collecting a client's personal information through service providers who are using the web-based portal as a client management system.	The Department decided that the client management functionality of the Data Exchange would be made available to service providers who report by way of a system to system transfer or bulk upload (see response to Recommendation 3). The standard notification in the 'Protecting Client's Privacy' of the Data Exchange Protocols was also amended to make it clear that: o the Department is making the Data Exchange available to the provider to be used as a client management system for the provider's own purposes, and that this involves the Department storing the client's personal information on the Data Exchange for access by the provider only; and o more information about privacy complaints can be found in the Department's privacy policy, published on the Department's website at https://www.dss.gov.au/privacy-policy.
7	Regularly assess the risk that the Department might be disclosing 'new' personal information about clients to service providers in the reporting context.	These risks are being managed through meetings of the report planning committee and/or other equivalent governance bodies which are expected to evolve over time. The terms of reference for the relevant committee will include endorsing all new reports, and the review of all new reports for privacy implications prior to endorsement.