

Ensuring client privacy on DEX within organisations

1. Purpose

The purpose of this resource is to improve client privacy within TEI funded service providers when using the Data Exchange.

2. Why

Feedback from the sector shows that although all TEI funded services must have policies that ensure client privacy as part of their funding agreement, the visibility of client information across outlets within the same organisation is a concern, particularly in smaller towns where clients may be more recognised and for highly sensitive cases.

3. Background

DEX was designed to ensure a client's personal information is protected through stringent protocols that comply with the requirements of the Privacy Act 1988, including the Australian Privacy Principles (APPs).

Some organisations choose to use DEX to collect and store personal information, whereas other organisations do not.

Regardless of the upload method used (web-based portal, bulk upload or system-to-system transfer); organisations must apply the DEX consent and notification arrangements if they intend to store personal information in the DEX.

Where an organisation stores personal information in DEX, only the organisation can access the personal information stored on DEX.

Strict IT security protocols prevent DSS staff from accessing personal information in this system for any purpose other than confirming that the privacy protocols are working correctly.

Funding agencies such as DCJ use de-identified data from DEX for program management, policy development, research, and evaluation activities for government.

DSS applies best practice data deidentification and aggregation methods when producing reports and information for these purposes, to ensure that a client cannot be identified or re-identified by other government departments or organisations.

See the [Privacy Impact Assessment](#) conducted by the Australian Government Solicitor which examined the Data Exchange's compliance with the Privacy Act.



4. Organisations using DEX to collect and store personal information

Organisations using DEX to collect and store personal information are considered to be using DEX as a “client records system” or “client management system”.

This means they need to see the client’s personal information in DEX for the purpose of managing their client records and the services being delivered to clients.

When reporting client-level records and using DEX as a client records system, the personal information that organisations submit to DEX (either through the web-based portal, bulk uploading of files or a system-to-system transfer) is stored by DSS on DEX. This includes the client’s name/pseudonym and address information.

Organisations who use DEX as a client records system must adhere to the [notification and consent requirements](#) (p11, DEX Protocols), which ensure that DSS complies with its obligations under the Privacy Act and the APPs.

To satisfy the notification requirements organisations must include the DSS standard notification on their registration forms, or ensure that the client is aware of those matters before the client’s personal information is entered on DEX or as soon as practicable.

5. Organisations NOT using DEX to collect and store personal information

The consent and notification arrangements do not apply to organisations if they choose not to store personal information in DEX.


For this purpose, organisations will indicate that client consent has not been provided when reporting through a system-to-system transfer or bulk upload.

The information that is stored in a client level unit record will not include the client’s name, pseudonym or street-level address.

6. Staff access to client information on DEX

Clients are entered once in DEX at the Organisation (ABN) level, and can then be added to Cases and Sessions according to the outlets and program activities they access, which saves a significant amount of time and resources by not having to re-enter clients.

Only DEX Org Administrators within the organisation can view all clients across the organisation.



Staff with Editor or View Only access can only see clients for the Outlets and Program Activities they have been given access to.

Clients within the organisation are searchable by staff in two ways:

- By clicking the 'client icon' under the 'Find menu'; or
- Typing the client's name or Client ID in the 'Go to' search box

When service providers generate a Standard or Partnership report in DEX, only the Client ID is visible, not the client's name.

7. Actions to ensure client privacy within TEI organisations

Actions recommended:


- TEI funded services and DCJ Districts should use the [TEI resources](#) available to reassure clients and staff that privacy is strictly maintained in DEX.
- TEI funded services should annually review their internal policies and procedures to help staff maintain client privacy.
- Org Administrators should set up their staff with Editor or View Only access so they only see the clients, for the Outlets and Program Activities they have been given access to. .
- TEI funded services may:
 - enter identifying client information in DEX to ensure high quality data is reported
 - untick the consent box to de-identify this information within the organisation (it's already de-identified externally)
 - use the 'Client ID' field to then search for clients in DEX; and
 - use a secure Client Management System that matches client information with DEX Client IDs.

Actions NOT recommended:

- Do not use pseudonyms and approximate DOBs for all clients as this leads to poor quality data and reduces learning for the organisation and the sector.
- Do not store client information insecurely eg paper files, computers without individual passwords; emails, spreadsheets, etc

8. Further information

- [Privacy Information Sheet](#) - will assist TEI service providers to understand the privacy obligations in their contract.
- [Using the Data Exchange: Consent and Privacy](#) - outlines the consent and privacy principles for using the Data Exchange
- [Example client intake form](#) - will assist TEI service providers to adhere to privacy obligations

- 
- Contact your DCJ Commissioning & Planning Manager (CPO)
 - Contact the TEI mailbox at tei@dcj.nsw.gov.au
 - [Data Exchange Protocols](#) – Main operational manual for users of the Data Exchange.
 - [Find and Edit a Client](#) – for guidance on how to find and edit a client in DEX.