Using the Data Exchange: Consent and Privacy

This document is for service providers funded under the following Department of Communities and Justice (DCJ) programs:

- Targeted Earlier Intervention (TEI)
- Family Connect and Support (FCS)
- Supporting Families into Early Childhood Education (SFiECE)

This document outlines the consent and data privacy principles your organisation must follow to use the Data Exchange.

These principles apply to all organisations who intend to store clients' **personal** information in the Data Exchange.

Service providers should use this information to inform their organisations privacy policy and to ensure their practices for collecting, using and disclosing client's personal information is lawful (see Privacy Information Sheet for more details).

Service providers are responsible for ensuring they obtain the correct consent and the necessary information is communicated to their clients.

Further resources:

- Privacy Information sheet: resource to assist TEI service providers to understand the privacy obligations in their contract. TEI service providers should use this information to inform their organisation's privacy policy and to ensure their practices for collecting, using and disclosing clients' personal and health information is lawful.
- The Data Exchange Protocols, Section 4: outlines the Data Exchange privacy protocols and organisation's privacy obligations.
- Example client intake form: resources to support service providers to adhere to their consent and privacy obligations. It includes the DSS standard notification on privacy and consent statements.

Frequently Asked Questions

Key consent and privacy principles

1. What is personal information?

Personal information is information about an individual that can be used to identify them. In the Data Exchange, personal information is the client's:

- first name
- last name
- street-level address (e.g. 1 Main Street)

Other information about clients, (e.g. date of birth, gender, Indigenous status, disability status) is also collected by organisations and reported into the Data Exchange. However, this is NOT personal information as it cannot be used to identify an individual.

Organisations must apply the Data Exchange consent and privacy arrangements if they intend to store **personal information** in the Data Exchange.

2. What are the key consent and privacy principles my organisation needs to follow?

If your organisation stores clients' personal information in the Data Exchange you must:

1	Use the DSS standard notification on privacy (or similar) to notify clients about the Data Exchange	See Question 3 and 4
2	Obtain consent to store clients' personal information in the Data Exchange	See Question 5
3	Obtain consent for clients to participate in follow up research, surveys, and evaluation	See Question 5

If your organisation stores clients' personal information outside of the Data Exchange, you must also:

4	Use a privacy notice to clearly communicate to clients how and why their information will be used	See Question 6
5	Obtain consent to collect, use and disclose clients' personal information	See Question 6

For more information about your organisation's privacy obligations see: Privacy Information Sheet. This will support you to better understand the privacy obligations in your DCJ contact.

3. What information do I need to give my clients about the Data Exchange?

All organisations who upload or enter clients' personal information in the Data Exchange must adhere to the notification and consent requirements in the Data Exchange Protocols.

This means you must include the **DSS standard notification on privacy** on your registration/intake forms.

You need to provide clients with this notification before their personal information is stored in the Data Exchange or as soon as possible after.

The DSS standard notification is outlined below:

> "The information that we collect from you on this form includes your personal information. Your personal information is protected by law, including by the Commonwealth Privacy Act.
>
> The client management system that we are using is an IT system called the 'Data Exchange'. This system is hosted by the Australian Government Department of Social Services (DSS). Your personal information that is stored by DSS on the Data Exchange will only be disclosed to us for the purposes of managing your case. You are not required to provide your personal information to DSS. If you do not consent to the collection of your personal information, this will not affect the services provided to you. If you provide your personal information to DSS, you can ask for this information to be removed by DSS at any time.
>
> DSS de-identifies and aggregates data in the Data Exchange to produce information for policy development, grants program administration, and research and evaluation purposes. This includes producing reports for sharing with organisations. This information will not include information that identifies you, or information that can be used to re-identify you, in any way.
>
> You can find more information about the way DSS will manage your personal information in DSS's privacy policy, which DSS has published on its website. This policy contains information about how you may access the personal information about you that is stored on the Data Exchange and seek correction of that information. This policy also includes the circumstances in which DSS may disclose personal information to overseas recipients, as well as information about how you may complain about a breach of the Australian Privacy Principles by DSS, and how DSS will deal with your complaint."

See Section 4.2.1 of the Data Exchange Protocols (pg. 12). This notification ensures DSS complies with its obligations under the Privacy Act.

Note: The DSS Standard Notification arrangements do not apply to organisations who choose not to store personal information in the Data Exchange (e.g. services who conduct system-to-system transfers). See Question 7.

4. Can I change the DSS standard notification on privacy?

You may use an alternative notification on privacy. However, it must include the following key information about the Data Exchange and its privacy principles – as required by the Australian Privacy Principles 5.2:

(a) the Data Exchange is an IT system that is hosted by DSS
(b) the organisation is using the Data Exchange for client management purposes, and the client's personal information is stored on the Data Exchange for this purpose only
(c) the client's personal information which is stored by DSS on the Data Exchange, is only visible to the organisation that collected the information for the purposes of managing the client's case
(d) DSS de-identifies and aggregates personal information that is stored on the Data Exchange to produce information for policy development, grants program administration, research and evaluation purposes, and this will not include information that identifies the client, or re-identifies the client, in any way
(e) DSS's privacy policy is published on its website. The website contains information about how the client may access or correct the personal information that is stored on the Data Exchange; complain about a breach of the APPs by DSS, and how DSS will deal with the client's complaint. The privacy policy also contains information about the circumstances in which DSS may disclose personal information to overseas recipients
(f) the consequences if personal information is not collected from the client (if any).

See Section 4.2.2 of the Data Exchange Protocols (pg. 12-13).

> **Translated DSS Standard Notification on Privacy**
>
> The DSS Standard Notification on Privacy has been translated into 14 different languages for clients. These translated documents are available on the Fams website: https://fams.asn.au/resources/tei-resources/

5. What consent do I need to collect when using the Data Exchange?

You must ask clients if they consent for the following:

a) Consent to have personal information stored in the Data Exchange

All service providers must obtain client consent before storing a client's personal information in the Data Exchange – asking for this consent is mandatory.

In the Data Exchange, personal information is the client's:

- first name
- last name
- street-level address (e.g. 1 Main Street)

This consent only applies to personal information. If a client does not consent you can still record other information about the client (e.g. gender, date of birth, cultural background, client outcome and satisfaction information).

Note: if you conduct bulk uploads or system-to-system transfers you may choose not to store client's personal information in the Data Exchange. See Question 7.

b) Consent to participate in follow up research, surveys, and evaluation

All service providers must ask clients if they consent to participate in follow up research, surveys, or evaluation - asking for this consent is mandatory.

Funding agencies (e.g. DCJ) and third parties (e.g. universities) are often interested in conducting research and evaluations to better understand client needs and how to improve the service system. This consent enables DSS to create a pool of potential participants for future research projects and evaluations.

> **Note:** Clients can consent to either, both or neither of these statements. One statement does not impact the other.
> See Question 10 for what to do if a client does not consent.

> **Note:** all clients with a statistical linkage key (SLK) will be included in the evaluation of the TEI program. If clients do not tick this box, it means they will be excluded from follow up questions only.
>
> See Question 27 and 28 for further information on SLKs

> See **Appendix 1. When I need to collect client consent?**

6. Does my organisation need to obtain consent if we store data outside of the Data Exchange?

Your service may have its own data collection and storage system. If you store client information outside of the Data Exchange (e.g. another IT platform, spreadsheets etc.) you must also obtain consent to store and use this information.

This is separate to the consent sought for using the Data Exchange.

See the TEI Privacy Information Sheet for information and advice about how to do this. This document will help you ensure your organisation's practices to collect, use and disclose client information comply with NSW and Federal privacy legislation.

---

7. What if my organisation chooses not to store personal information in the Data Exchange?

If your organisation conducts bulk uploads or system-to-system transfers, you may choose to not store client's personal information in the Data Exchange.

To do this, you will:

- remove clients' personal information (i.e. full name and street-level address) before your upload or transfer.
- indicate client consent has not been provided
- generate SLKs for your clients

The DSS Standard Notification arrangements do not apply to your organisation if you choose not to store clients' personal information in the Data Exchange.

However, we still encourage you to speak to your clients about the reporting platform. While it is not a legal obligation, service providers should be open and honest with their clients about who is using their information (even if it is de-identified) and why.

Further, service providers will still need to seek consent to participate in follow-up research, surveys, or evaluation (See Question 5, Part B).

> **See Appendix 1. When I need to collect client consent?**

Obtaining consent and recording client's information

8. Which clients do I need to obtain consent from?

You only need to ask individual clients for consent.

You do not need to obtain consent from unidentified client groups. This is because we do not store their personal information in the Data Exchange. We only record the number of unidentified people who attended a session.

---

9. What's the difference between individual and unidentified group clients?

In the Data Exchange, we can record clients as individual clients or as unidentified group clients (see Table 1).

Individual clients have a client record created in the Data Exchange. They can be identified or de-identified.

Unidentified group clients are people who participate in large group events and it's not practical or possible to record their details.

Table 1. Individual clients and unidentified group clients

Individual clients: Clients who have a client record created for them in DEX		Unidentified group clients: Clients who are unknown to the service
Identified clients Clients have consented to have their personal information stored in the Data Exchange.	**De-identified clients** Clients have NOT consented to have their personal information stored in the Data Exchange.	Clients who participate in large group activities Note: they may also be clients who refuse to disclose any information about themselves (see Question 12 and 13).
Services should try to record individual clients when it is practical and possible. Some examples include: o Small group activities o Playgroups o Counselling o Parenting programs o Home visits/Case management o Mens/Womens/Youth/Parenting groups o School programs De-identified clients still have a client record – it's just de-identified. Services need to use the Client ID, instead of the client's name, to attach them to the services they participate in. De-identified clients still count towards your client totals.		Unidentified groups are recorded if it is not practical or possible to collect individual client information. Some examples: o A community event o A one-off information session o Info/advice/referral in a community centre o Interagency meeting Clients who refuse to provide any information about themselves when participating in one-on-one or small group activities (i.e. anything in the left hand column) can recorded as unidentified clients.

10. What happens if a client does not give consent to have their personal information stored in DEX?

When consent is not given, the client's personal information cannot be stored in the Data Exchange. Table 2 describes what to do if a client does not give consent.

Table 2. What happens if a client does not give consent?

For service providers using the web-based portal

1. Create a client record for the client – enter all the information you have about the client (including their name and address).
2. Untick the 'consent to store personal information' box in the client record. This will de-identify the client record (see Figure 1). The client's name and street-level address will be hidden and not stored in the Data Exchange.
3. Keep a record of the Client ID. You will not be able to search for the client by their name in the Data Exchange. You will have to use their Client ID to find them. You will need the Client ID to attach the client to the cases and sessions they attend, to record SCOREs and to update their client record as needed.

For service providers conducting bulk uploads/transfers

1. Use the 'false' value in your data file.
2. Generate a SLK or configure your existing system to push SLKs across to the Data Exchange.
3. Remove clients' personal information from your XML file or system before uploading it to the Data Exchange.

Figure 1. De-identified client records in the Data Exchange
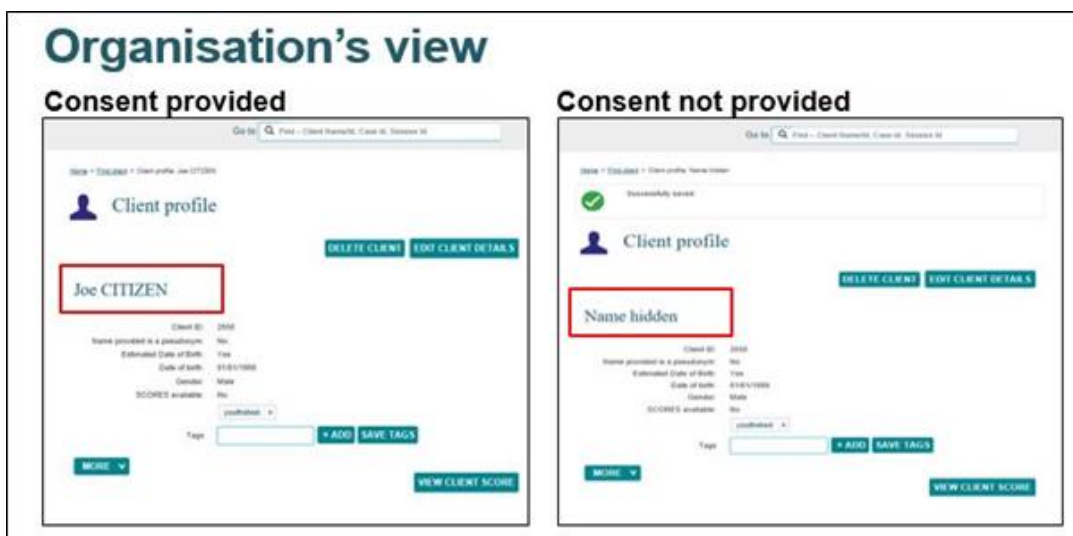
See [Appendix 2: Client Consent Cheat Sheet](#)

11. What happens if a client does not give their personal details?

You can still create a client record for a client who does not disclose their personal details. The client can:

Use a pseudonym: If a client does not wish to disclose their real name, they can use a pseudonym (a false name) instead. In the client record, tick the box to indicate that pseudonym is being used (see Figure 2).

The client should use this pseudonym for the duration of the service.

Use an estimated date of birth: If a client does not know or does not wish to disclose their date of birth, you can record an estimate. This is just a year of birth. It should be as close to the client's age as possible.

In the client record, tick the box to indicate that their date of birth is estimated (see Figure 2).

Figure 2. Options to record client details

For all other information in the client record (e.g. gender, Indigenous status), record the information the client provides. If client does not provide certain information, leave it blank.

> **Note:** It is very important that you do not enter false client details in the Data Exchange. False or incorrect client details will compromise the quality of our data. It will also mean we're not able to capture a client's journey through the service system.

See Appendix 2: Client Consent Cheat Sheet

12. What happens if a client will not give any information about themselves?

If a client refuses to provide any information about themselves you can:

a) Create an individual client record using a pseudonym

Create a client record for the client. Leave any unknown demographic fields blank.

Use a pseudonym for the client. In the client record, tick the box to indicate that pseudonym is being used (see Figure 2).

Untick the consent boxes to say that consent has not been given.

Keep a record of the Client ID. You will not be able to search for the client by their name in the Data Exchange. You will have to use their Client ID to find them. You will need the Client ID to search for the client to attach them to the cases and sessions they attend, to record SCOREs and to update their client record as needed.

Over time, as you build a relationship with the client, you could try to populate the client record with any information they provide. If they do not provide any information, ever, that's ok too. Just leave the client record empty.

b) Record the client as an unidentified client

You can record the client as an unidentified client.

Create cases and sessions as you would for any client. Record the client as 1 unidentified client in the relevant cases and sessions.

Over time, as you build a relationship with the client, you could try to create a client record with any information they provide. If they do not provide any information, ever, that's ok too. Just continue recording them as an unidentified client.

Recording the client this way, means that you will NOT be able to record Circumstance, Goals or Satisfaction SCORE for them.

---

13. What happens if a client doesn't want any information about them stored in the Data Exchange?

You can record the client as an unidentified client.

Create cases and sessions as you would for any client. Record the client as 1 unidentified client in the relevant cases and sessions.

Recording the client this way, means that you will NOT be able to record Circumstance, Goals or Satisfaction SCORE for them.

See Appendix 2: Client Consent Cheat Sheet

14. What is a pseudonym and when should I use one?

A pseudonym is a fake or 'made up' name. If an individual client does not wish to disclose their real name, they can use a pseudonym. In the client's record, you can indicate that a pseudonym has been used (see Figure 2, pg. 11).

Only use a pseudonym if a client does NOT disclose their real name.

The client should use that same pseudonym for the duration of service delivery.

Note: a pseudonym is NOT a shortened or modified version of a client's real name. For example, 'Bill' for William or 'Kate' for 'Katherine'. A client's full name should be used in their client record.

15. Can children, young adults or someone with compromised capacity give consent?

For a child, it is best practice to seek consent from their parent or guardian.

However, if you determine a child or young person fully understands what they are consenting to, you can get their consent directly.

DSS propose a general rule: a young person aged 15 and over has the capacity to consent, unless there is something to suggest otherwise. Children and young people aged under 15 are presumed not to have capacity to consent.

You may have clients whose capacity to consent is compromised (e.g. people with disabilities). You may have to implement special practices. You should use your professional experience to determine the best way to obtain consent. For example, a guardian may provide consent on behalf of a client.

16. What happens when a client does not have the capacity to give consent?

Organisations should use their professional judgement to assess whether a client is capable of giving informed consent. See also question 15.

If you determine that a client does not have the capacity to consent, and there is no one to provide consent on their behalf, you should assume that consent has not been given. See Question 10.

17. What happens if a client changes their mind about consent?

A client can change their mind about consent at any time.

If a client withdraws consent, update their client record in the Data Exchange. See Question 10.

If a client agrees to consent, update their client record in the Data Exchange.

18. What happens if lots of my clients do not consent? Will this impact my data quality?

No. This will not impact the quality of your data.

When a client does not consent to have their personal information stored in the Data Exchange, the system de-identifies the client by removing their name and street-level address.

They are still recorded as an individual client in the Data Exchange and they still count towards your client totals.

19. How often do I need to get consent?

You only need to obtain consent once.

However, if a client attends your service over a long period of time, you should check in with the client to ensure they have not changed their mind about consent.

If an individual client participates in multiple activities/services you provide, your organisation only needs to obtain consent once. This is because the client only has one Client ID with their information stored in the Data Exchange.

However, you should check in with the client when they participate in a new activity/program to ensure they have not changed their mind about consent.

A client cannot provide consent for one activity and withdraw consent for another. If a client withdraws consent for any activity, you should update their record in the Data Exchange to reflect this. If this happens, please talk to your client about the Data Exchange and consent to ensure they understand what they are consenting to.

20. Can I obtain consent verbally?

Yes. You can obtain consent verbally (e.g. over the phone or online).

You should keep a record of this. For example, on your client intake form, note consent was given over the phone and the date it was given.

---

21. I've already entered a client's personal information in the Data Exchange, but I didn't obtain consent. What should I do?

Don't panic. You can obtain client consent retrospectively.

You should try to obtain consent as soon as possible.

If you are not able to obtain consent quickly (e.g. 1 week) we recommend unticking the consent boxes in the client's record in the Data Exchange. See Question 10.

When you have the opportunity to ask your client about consent, you can update their record in the Data Exchange to reflect their decision (i.e. if they have provided consent, tick the boxes. If they did not give consent, leave them unticked).

Privacy protocols and practices

22. What privacy protocols does DSS have in place?

The Data Exchange was designed to ensure a client's personal information is protected through stringent protocols that comply with the Privacy Act 1988.

DSS must comply with its obligations under the Privacy Act 1988 when storing personal information from clients.

When you store personal information in the Data Exchange, only your organisation has access to it. Strict IT security protocols prevent DSS staff from accessing personal information for any purpose other than confirming that the privacy protocols are working.

Information stored in the Data Exchange is de-identified. This means DCJ and DSS cannot see a client's personal information.

23. Who can enter and see data in the Data Exchange?

Any staff member in your organisation who has access to the Data Exchange will be able to see clients' information.

Staff in your organisation can only see the case and session details for the outlets and program activities they have been assigned. See Add and edit a user for more information.

It is the responsibility of service providers to ensure they have privacy practices in place that prevent client information from being misused.

24. How does the Data Exchange de-identify clients?

In all cases, data submitted to the Data Exchange is de-identified.

De-identification means removing all identifying information so a person's identity can no longer be 'worked out'.

The Data Exchange de-identifies client data by:
- using a Statistical Linkage Key (SLK) (see Question 27)
- data aggregation: data is presented in a summarised format, rather than on a record-by-record basis.

Government use of Data Exchange data

25. How do DSS use the information stored in the Data Exchange?

DSS can only access de-identified information stored in the Data Exchange. This means they cannot see a client's personal information.

DSS use data stored in the Data Exchange for policy development, grants program administration, and research and evaluation. This includes producing reports for other organisations. They may link this information with other data sources (e.g. data collected from other government departments).

DSS do not link Data Exchange data to track if people provide the correct information to the Australian Government. They do not use the data to verify personal information provided by people about their circumstances, status or relationships. For example, Data Exchange data is not compared to Centrelink data to see if people provide the same or correct information.

See also Question 29.

---

26. How do DCJ use the information stored in the Data Exchange?

DCJ can only access de-identified information stored in the Data Exchange. This means they cannot see a client's personal information.

DCJ will use the data to monitor a service provider's performance and ensure they adhere to their contract. The data is used to ensure service levels are reached and client outcomes are achieved.

DCJ will also use the data to evaluate early intervention programs (e.g. TEI, SFiECE, FCS). The data is used to assess the effectiveness of the programs and to determine if and how the programs improve client outcomes. DCJ will use this information to improve programs and how NSW government responds to client and community needs.

When DCJ evaluates the early intervention programs they are only interested in aggregated data. No results for individual clients will be reported.

---

27. What is a Statistical Linkage Key?

A Statistical Linkage Key (SLK) is a 14 character algorithm generated from a client's first and last name, gender, and date of birth. An SLK looks like this: MIHOH140219711

SLKs de-identify client records. They are used to link two or more records belonging to the same client. This enables us to capture a client's journey through the service system without disclosing the identity of the individual client.

This means when we link our data with other datasets (e.g. Child protection, Justice) a client's identity is never revealed or disclosed. SLKs make sure DSS and DCJ cannot see a client's personal information.

An SLK will be invalid if client details (name, date of birth and gender) are false, incomplete and incorrect. They will also be invalid if they are recorded differently across organisations (e.g. John vs. Jonathon). If a client returns to a service or moves between services, it will get harder to follow their journey over time. As such, it is very important that you do not enter false client details into the Data Exchange.

28. Do I need to generate a SLK?

For organisations using the Data Exchange web-based portal, the SLK is automatically generated within the system.

For organisations using bulk uploads or system-to-system transfers, the SLK can be incorporated into your client management system.

Go to [The Data Exchange Web Services technical specifications](#) for help configuring your system to transfer the SLK across to the Data Exchange.

29. Can client data be linked to other datasets (e.g. child protection data, Centrelink data)?

Yes, client data can be linked to other datasets, including Commonwealth datasets and NSW Government datasets.

When this occurs all of the data is de-identified. SLKs are used to link the client records. This means, DCJ and other government departments (e.g. DSS) will not know who the information is about.

Analysis of linked data also occurs at an aggregate level. This means, we do not look at individual clients, but at large groups across the state or country. For example, we can use linked datasets to answer questions like:

- What percentage of children in the TEI program are coming into contact with the child protection system?

- What percentage of clients in the TEI program receive a welfare payment?

Data linkage supports us to understand client needs and what combination of services lead to the best results for clients. It also enables us to analyse client pathways within and across government departments and programs. It includes looking at client pathways through the service system, across multiple organisations and services.

DSS is exploring how it could share this aggregate data with organisations.

30. What does privacy legislation say about using the data to evaluate the TEI program?

Section 17 of the [Personal Information Protection Act 1998](#) (PPIP Act) stated as follows:

---

17 Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless —

a) the individual to whom the information relates has consented to the use of the information for that other purpose, or
b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or
c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

Guidance from the Privacy Commissioner indicates that program evaluations and audits are examples of directly related secondary purposes; as they are deemed to be for lawful purposes directly related to the functions or activities of the agency. The [Privacy Commissioner's Statutory Guidelines on Research](#) section 27B states:

> The assessment or program evaluation of the operation of the agency or services provided by the agency are generally not categorised as research as they are deemed to be for lawful purposes directly related to function or activity of the agency.

Appendix 1. When do I need to collect client consent?

Use the flow charts to help you understand when to obtain client consent.
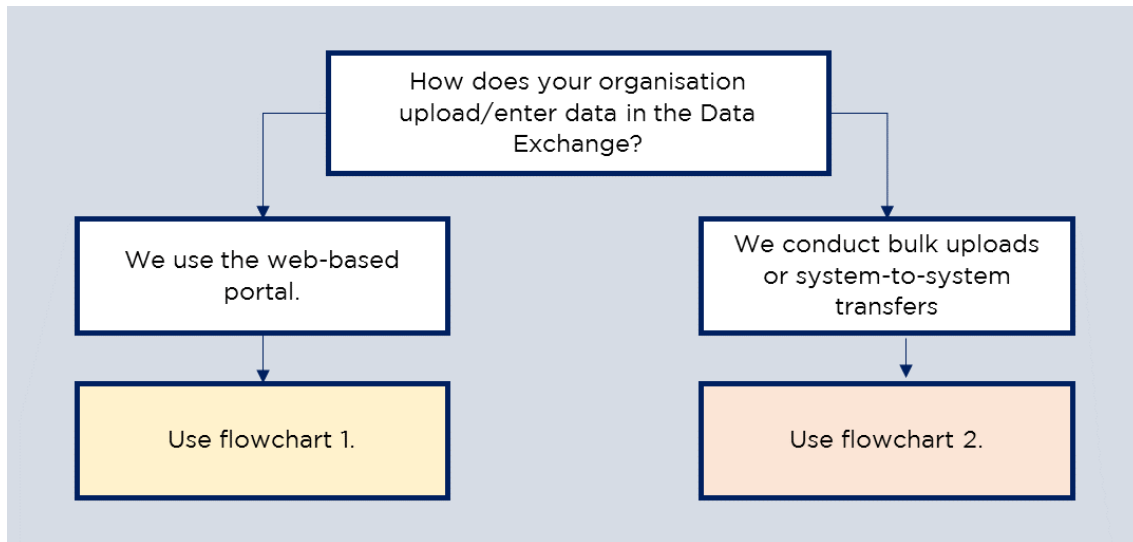
Flow chart 1: For organisation who use the web-based portal

CONSENT 1

Include the DSS Standard Notification on Privacy or an alternative notification in your registration/intake forms

↓

Obtain client consent to store client's personal information in the Data Exchange

↓

Does the client have the capacity to consent?

Yes → Does the client give consent?

No → Personal information cannot be stored in the Data Exchange.

Untick the consent to store personal information box. Keep a record of Client ID.

Does the client give consent? **No** → (Personal information cannot be stored in the Data Exchange. Untick the consent...)

Yes → Personal information can be stored in the Data Exchange. Tick consent to store personal information.

CONSENT 2

Obtain client consent to participate in follow up research, surveys and evaluation

↓

Does the client have the capacity to consent?

Yes → Does the client give consent?

No → Untick the consent to participate in follow up research box.

Does the client give consent? **No** → (Untick the consent to participate in follow up research box.)

Yes → Tick consent to participate in follow up research.

CONSENT 3

Does your organisation store client's personal information outside the Data Exchange? E.g. in your own client management system, spreadsheets or other documents.

Yes → Your organisation must also obtain client consent to store and use client's personal information.

This is separate to the consent sought for using the Data Exchange.

You must ensure your practices to collect, store and use client information comply with privacy legislation as outlined in Clause 19 of the Human Services Agreement.

See Question 5 for more information.

No → You only need to obtain Consent 1 and Consent 2, as outlined above.

Flow chart 2: For organisations who conduct bulk uploads or system-to-system transfers

CONSENT 1

Does your organisation intend to store client's personal information (i.e. name and address) in the Data Exchange?

Yes / **No**

Yes → Include the DSS Standard Notification on Privacy or an alternative notification in your registration/intake forms

↓

Obtain client consent to store client's personal information in the Data Exchange

↓

Does the client have the capacity to consent?

No → (to Personal information cannot be stored box)

Yes ↓

Does the client give consent?

No → (to Personal information cannot be stored box)

Yes ↓

Personal information can be stored in the Data Exchange. Tick consent to store personal information.

No → If your organisation conducts bulk uploads/transfers you can choose not to store client's personal information in the Data Exchange. To do this, you must:
- remove client's personal information before you conduct your upload/transfer.
- indicate client consent has not been provided.
- generate SLKs for your clients.
You do not need to obtain consent from clients.

Personal information cannot be stored in the Data Exchange.

Use the 'false' value in your data file. Remove client's personal information before your upload/transfer. Generate a SLK.

CONSENT 2

Obtain client consent to participate in follow up research, surveys and evaluation

↓

Does the client have the capacity to consent?

Yes ↓ / **No →**

Does the client give consent?

No → Use the 'false' value in your data file.

Yes ↓

Tick consent to participate in follow up research.

CONSENT 3

Your organisation must obtain client consent to store and use client's personal information.

This is separate to the consent sought for using the Data Exchange.

You must ensure your practices to collect, store and use client information comply with privacy legislation as outlined in Clause 19 of the Human Services Agreement.

See Question 5 for more information.

Appendix 2. Using the Data Exchange: Client consent cheat sheet

Client consents to have **personal information** stored in the Data Exchange	1. Create a client record for the client – enter all the information you have about the client.
	2. Make sure the consent box is ticked.
	3. You can search for the client using their name or Client ID. • Attach the client to relevant Cases and Sessions. • Record SCOREs for the client as necessary.

Client does NOT consent to have **personal information** stored in the Data Exchange	1. Create a client record for the client – enter all the information you have about the client (including their name and address).
	2. Untick the 'consent to store personal information' box. • This will de-identify the client record (see Figure 1). • The client's name and street-level address will be hidden. They will be not stored in the Data Exchange.
	3. Keep a record of the Client ID. • You will not be able to search for the client by their name in the Data Exchange. You will have to use their Client ID to find them. • You will need the Client ID to search for the client to attach them to the cases and sessions they attend, to record SCOREs and to update their client record as needed.

Client does not provide personal details (e.g. name, DOB)	1. Create a client record for the client – enter all the information you have about the client. Leave an unknown demographic fields blank.
	2. If a client does not disclose their real name, they can use a pseudonym (a false name) instead. In the client record, tick the box to indicate that pseudonym is being used (see Figure 2). • The client should use this pseudonym for the duration of the service.
	3. If a client does not know or does not wish to disclose their date of birth, you can record an estimate. In the client record, tick the box to indicate that their date of birth is estimated (see Figure 2). • This is just a year of birth. It should be as close to the client's age as possible.
	4. Untick the 'consent to store personal information' box.
	5. Keep a record of the Client ID. • You will not be able to search for the client by their name in the Data Exchange. You will have to use their Client ID to find them. • You will need the Client ID to search for the client to attach them to the cases and sessions they attend, to record SCOREs and to update their client record as needed.

Client does not provide any information about themselves	Option A.	1. Create a client record for the client. Leave an unknown demographic fields blank.
		2. Use a pseudonym. In the client record, tick the box to indicate that pseudonym is being used (see Figure 2).
		3. Untick the 'consent to store personal information' box.
		4. Keep a record of the Client ID. • You will not be able to search for the client by their name in the Data Exchange. You will have to use their Client ID to find them. • You will need the Client ID to search for the client to attach them to the cases and sessions they attend, to record SCOREs and to update their client record as needed.

		5. Over time, as you build a relationship with the client, you could try to populate the client record with any information they provide. If they do not provide any information, ever, that's ok too. Just leave the client record empty.
	Option B.	1. Record the client as an unidentified client. Create cases and sessions as you would for any client and just record the client as 1 unidentified client in the relevant cases and sessions.
		2. Over time, as you build a relationship with the client, you could try to create a client record with any information they provide. If they do not provide any information, ever, that's ok too. Just continue recording them as an unidentified client. • Recording the client this way, means that you will NOT be able to record Circumstance, Goals or Satisfaction SCORE for them.

Client does not want any information about them stored in the Data Exchange	Record the client as an unidentified client. Create cases and sessions as you would for any client and just record the client as 1 unidentified client in the relevant cases and sessions.

Figure 1. De-identified client records in the Data Exchange

Figure 2. Options to record client details