October 2020

Using the Data Exchange: Consent and Privacy

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

These principles apply to all Targeted Earlier Intervention (TEI) organisations who intend to store clients' **personal** information in the Data Exchange.

Also see:

- 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.
- 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 organisations privacy policy and to ensure their practices for collecting, using and disclosing client's personal and health information is lawful.

Frequently Asked Questions

1. What are the key consent and privacy principles my organisation needs to follow? 3
2. What is the DSS standard notification on privacy? 4
3. Can I change the DSS standard notification on privacy? 5
4. What consent do I need to collect when using the data exchange? 5
5. Does my organisation need to obtain consent if we store data outside of the data exchange? 6
6. Which clients do I need to obtain consent from? 7
7. What happens if a client does not give consent? 8
8. What happens if a client changes their mind about consent? 9
9. What happens if a client will not give their details? 9
10. Can children, young adults or someone with compromised capacity give consent? 10
11. What happens when a client does not have the capacity to give consent? 10
12. What happens if my clients do not consent? Will this impact my data quality? 10
13. How often do I need to get consent? 10
14. Can I obtain consent verbally? 11
15. What if my organisation chooses not to store personal information in the data exchange? 11
16. I've already entered a client's personal information in the Data Exchange, but I didn't obtain consent. What should i do? 12
17. What privacy protocols does DSS have in place? 12
18. Who can enter and see data in the data exchange? 12
19. How do DSS and DCJ use the information stored in the data exchange? 12
20. What is a statistical linkage key? 13

Appendix 1. Flow chart for storing individual clients' personal information in the data exchange 14

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

a) 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 2 and 3
2	Obtain consent to store clients' personal information in the Data Exchange	See Question 4
3	Obtain consent for clients to participate in follow up research, surveys, and evaluation	See Question 4

The Data Exchange was designed to ensure a client's personal information is protected through stringent protocols that comply with the Privacy Act 1988. Organisations must apply the Data Exchange consent and notification arrangements if they intend to store personal information in the Data Exchange.

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

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

b) If your organisation stores client's 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 5
5	Obtain consent to collect, use and disclose client's personal information	See Question 5

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

2. What is the DSS standard notification on privacy?

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 (see Section 4.2).

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 14.

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.

3. 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).

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

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 14.

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 and third parties (e.g. universities) are often interested in conducting research 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.

Researchers will contact organisations before any research activities start. Researchers will not be able to contact clients directly.

If a client consents to participate in follow up research, they are not obligated to participate in any projects. They can change their mind about consent at any time.

Note: Clients can consent to either, both or neither of these statements. One statement does not impact the other.
See Question 7 for what to do if a client does not consent.

5. 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 organisations practices to collect, use and disclose client information comply with privacy legislation.

---

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

In the Data Exchange, we can record information for individual clients or unidentified group clients.

You only need to obtain consent from your individual clients.

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.

Individual clients	Unidentified group clients
An individual person who has/will have a client record created in the Data Exchange. This client record includes their personal information. Individual clients are people who receive a service under the TEI program that is expected to lead to a measureable outcome.	A group of people who have received a service under the TEI program. No identifying information is collected from these clients.

7. What happens if a client does not give consent?

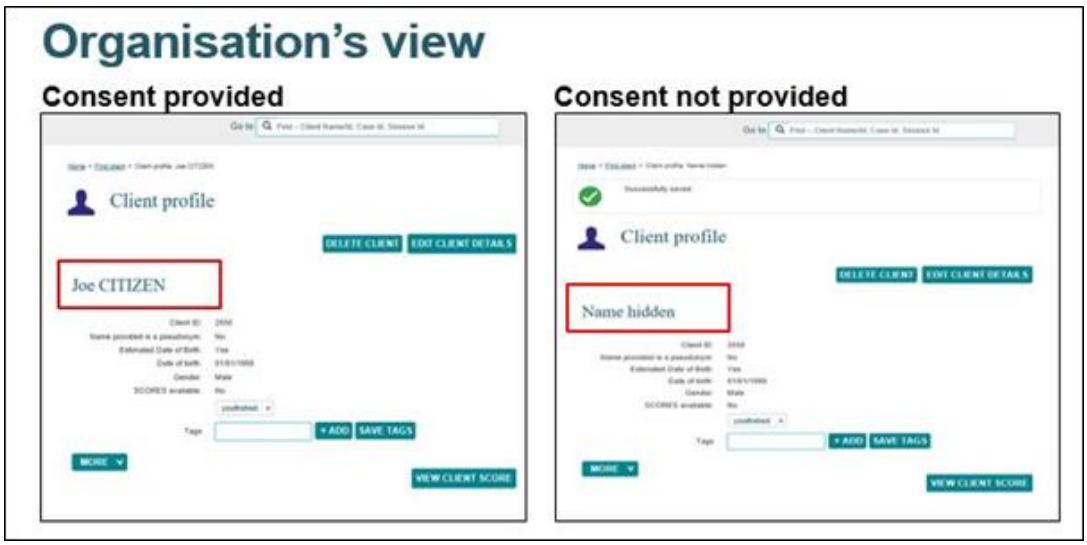
When consent is not given, the client's personal information is not stored in the Data Exchange. Table 1 describes what to do if a client does not give consent.

Table 1. What happens if a client does not give consent?

	Consent to store personal information in the Data Exchange	Consent to participate in follow-up research, surveys, and evaluation
For service providers using the web-based portal	Untick the 'consent to store personal information' box in the client's record. The client's name and street-level address will not be stored in the Data Exchange. You must still enter this information in the client's record so a Statistical Linkage Key (SLK) can be generated. You must keep a record of the client's Client ID. This will enable you to update the client's information as they continue to participate in your service (e.g. to add additional SCOREs). 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.	Untick the 'consent to participate in follow-up research' box in the client's record.
For service providers conducting bulk uploads or system-to-system transfers	Use the 'false' value in your data file. You must generate a SLK or configure your existing system to push SLKs across to the Data Exchange. You can remove a client's personal information from your XML file or system before uploading it to the Data Exchange.	Use the 'false' value in your data file.

When a client does not give consent for their personal information to be stored in the Data Exchange, their client record is de-identified. See Figure 1.

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



8. 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, you need to update their client record in the Data Exchange. See Question 6.

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

9. What happens if a client will not give their details?

If a client does not wish to disclose their 'real name', they can use a pseudonym (a false name) instead. The client should use this pseudonym for the duration of the service.

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

It is very important that organisations do not enter false client details in the Data Exchange. The Data Exchange uses client details (name, date of birth and gender) to generate SLKs (see Question 20).

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.

10. 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.

---

11. 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 9 above.

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 6.

---

12. 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.

Other information about the client will still be in your dataset (e.g. the activities they participated in and the outcomes they achieved).

Also see Question 7: What happens if a client does not consent?

---

13. 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.

14. 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.

15. 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 4, Part B).

16. 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. 1-2 weeks) we recommend unticking the consent boxes in the client's record in the Data Exchange. See Question 7.

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).

---

17. What privacy protocols does DSS have in place?

DSS must comply with its obligations under the Privacy Act 1988 when collecting 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.

---

18. 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.

19.How do DSS and DCJ use the information stored in the Data Exchange?

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

DCJ may use information stored in the Data Exchange to help improve how the NSW government responds to client and community needs. DCJ are interested in trends across the NSW state, not individual people. They cannot access information that will reveal a client's identity.

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).

20. 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

This means that a client's personal information is de-identified. DSS will not see a client's personal information, even when they consent to have their personal information stored on the Data Exchange.

SLKs enable us to capture a client's journey through the service system without disclosing the identity of the individual client. They can link two or more records belonging to the same client.

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.

A client's SLK is not visible to organisations in the Data Exchange. SLKs are only visible to a restricted number of DSS employees who perform database administration or data analytics.

Do I need to generate a SLK?

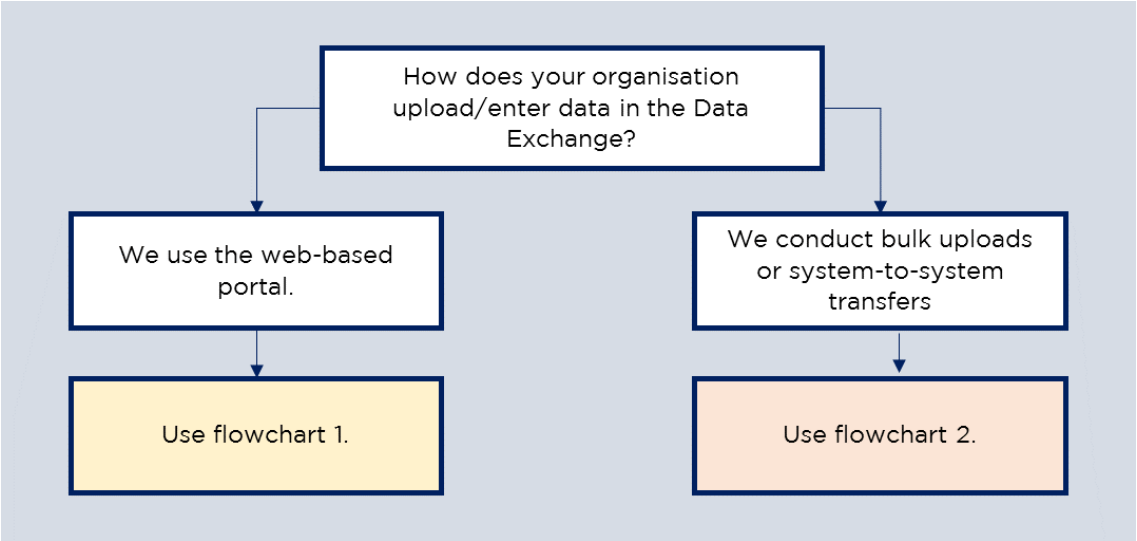
For organisations using the Data Exchange web-based portal, the SLK is automatically generated within the system.

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.

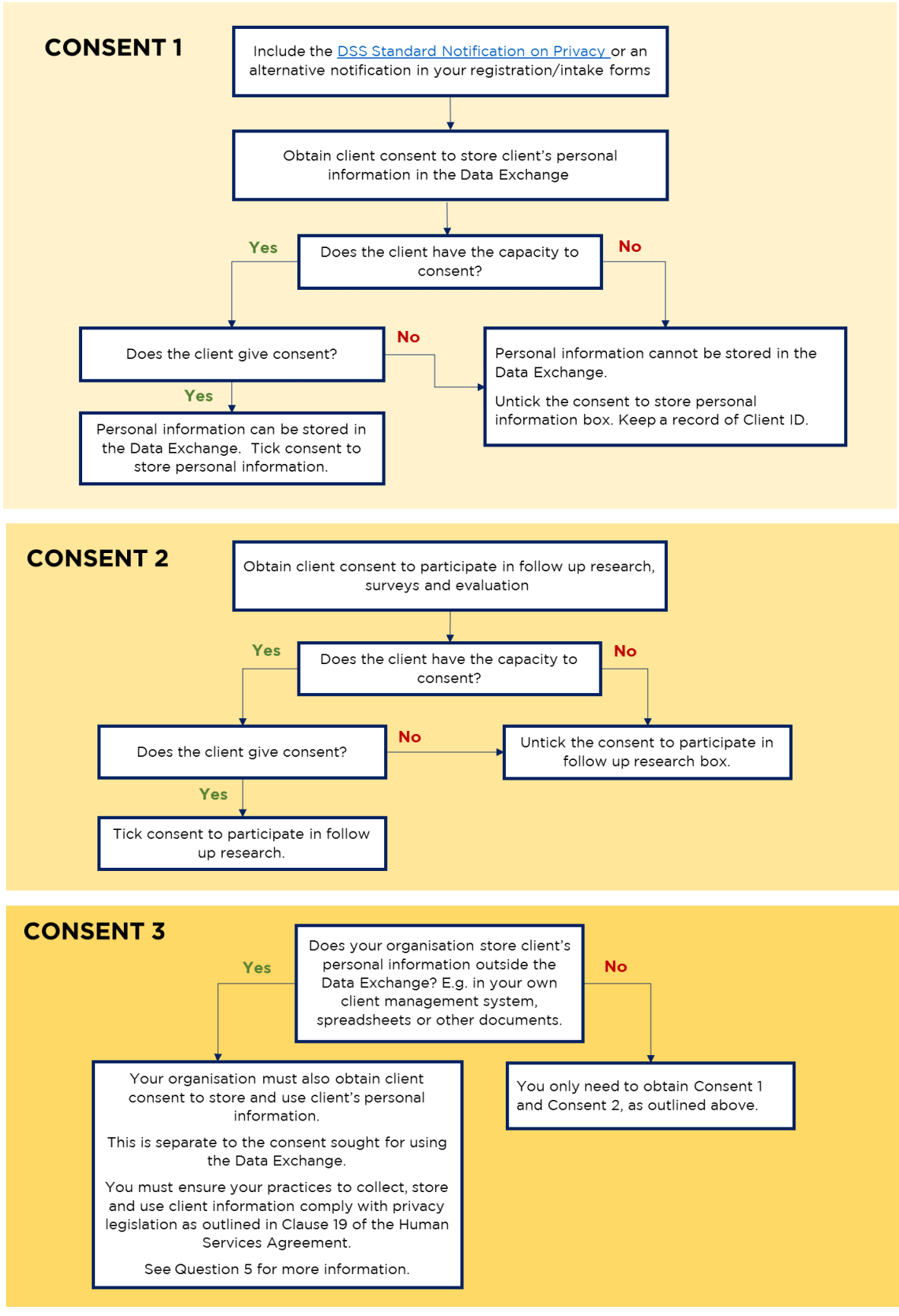
Appendix 1. Flow chart for storing individual[1] clients' personal information in the Data Exchange

Use the flow charts to help you understand when to obtain client consent.



[1] Note: Unidentified group clients do not need to provide consent.

Flow chart 1: For organisation who use the web-based portal



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