Australian Government
Department of Social Services

The Data Exchange Protocols for the Commonwealth Home Support Program (CHSP)

July 2025

Contents

Introduction

1.1 Purpose of this document

This document provides operational guidance to users of the Data Exchange who deliver the Commonwealth Home Support Program (CHSP) on behalf of the Department of Health, Disability and Ageing (DoHDA). The Data Exchange Protocols (CHSP) (the CHSP protocols) should be read in conjunction with the:

- Data Exchange Framework which outlines the principles and vision underpinning the Data Exchange
- Program Specific Guidance for organisations, which outline specific reporting requirements for each program
- organisation's funding agreement
- task cards and e-Learning modules for users of the Data Exchange web-based portal
- Data Exchange technical specifications for all users submitting their data through system-to-system transfer or bulk upload from their own case management software.

The protocols are not intended to prescribe how organisations should run their business or collect data; they are intended to provide practical information for managers and front-line staff to help them integrate the Data Exchange data definitions and requirements into existing service and administrative practices.

The protocols are periodically updated to provide current and accurate guidance.

1.2 The Data Exchange Framework

The Data Exchange requirements for CHSP providers are divided into two parts: a small set of mandatory priority requirements, and an extended data set, known as the partnership approach.

This approach to reporting is streamlined, automated and includes a shift in focus of performance measurement from 'outputs' to more meaningful information about service delivery 'outcomes' through:

- **Free access to a web-based portal**— Organisation can access a free IT system to manually input client data. This helps record clients, service and outcomes data that meet funding agreement performance data requirements and allows organisations to confidentially manage their core client and case information.
- **Bulk uploading and system-to-system transfers**—The Data Exchange supports organisations who have a compatible case management software to transfer information directly from their own systems through bulk uploading and system-to-system transfers.
- **Promoting a partnership approach to reporting**—Organisations participating in the partnership approach to share client outcomes data with their funding agency in exchange for relevant reports. These reports are outcomes focused and include a rich set of added information to help inform service delivery using program performance, client survey and government data.

Go to the Data Exchange website for more information about the Data Exchange's policy principles and program specific guidance.

2 Data Exchange organisation and user responsibilities

Organisations reporting into the Data Exchange are responsible for implementing appropriate controls and processes to:

- promote awareness of, and compliance with, the Data Exchange Protocols by users within the organisation; and
- obtain accurate, complete, unbiased and secure collection and recording of client, service delivery and outcome (where relevant) data in the Data Exchange.

Taking obligations under the *Privacy Act 1988* into account, organisations and users must make best endeavours to ensure data entered in the Data Exchange is, to the best of their knowledge:

- **Accurate** and up to date - it is the user's responsibility to correct or delete any incorrect data where possible, as soon as practicable, after becoming aware of any issues
- **Complete** – best efforts should be made to collect required data from clients and ensure all collected data is correctly entered into the Data Exchange
- **Unbiased** - data entered should:
    - be representative of the client population and free from avoidable sampling bias (for example, if 50% of clients identify as male, then close to 50% of SCORE assessments should be for male clients)
    - be objective and free from observer bias (for example, SCORE assessment data should reflect the most objective view of the client's circumstances possible and be free, as possible, from the assessor's personal opinion).
- **Secure –** client information should be protected from unauthorised use or disclosure, in accordance with Chapter 5 of the protocols.

Processes and controls implemented by organisations to ensure users meet their Data Exchange responsibilities may include (but are not limited to):

- Staff who use Data Exchange have read and agreed to adhere to the Data Exchange Protocols
- Staff who use Data Exchange have completed relevant online Data Exchange training
- Data entry and access rights to Data Exchange (and any third-party software product used to transfer data to Data Exchange) are periodically reviewed and remain appropriate
- Processes (e.g. written guidance to support how data is collected and recorded) have been established to ensure mandatory Data Exchange data is collected and accurately recorded (in any third-party software product or directly into the Data Exchange web-based portal)
- Processes (e.g. written guidance to support how data is collected and recorded) have been established to ensure SCORE data is accurate, complete and unbiased when recorded in Data Exchange
- Quality assurance processes have been established to confirm data transfers/uploads into Data Exchange are completed successfully (and any upload errors rectified)
- Any other processes and controls relevant to promoting compliance with the Data Exchange Protocols and data integrity.

CHSP funded organisations may be required, upon request by DoHDA, to provide evidence of processes and controls used to meet their Data Exchange responsibilities. DoHDA may request to visit their funded organisations' premises to observe these processes in practice. Funded organisations are responsible for ensuring any delivery partners (such as subcontractors, community partners, consortium members or brokers) using the Data Exchange also meet their Data Exchange responsibilities.

3 Recording client level data

This section describes the important concepts and terminology associated with collecting and reporting client level data. It is important that managers and front-line staff understand these concepts because they underpin the framework of the Data Exchange.

3.1 Client level data

Client level data refers to data collected and reported on each individual client rather than as summary (aggregate) data. The Data Exchange is designed to capture individual client level data. However, where collecting client data is not practical or possible, such as an activity involving a large group of people or a whole community, aggregate reporting is still accommodated by the system.

The main advantages of client level data are the:

- flexibility to analyse and report administrative data in multiple formats for different audiences, without burdening organisations with multiple data requests
- improved reliability of administrative data, as all organisations collect the same raw data records without the need to apply complex counting rules
- improved usefulness of administrative data, due to the use of a Statistical Linkage Key (SLK) allowing for the matching of de-identified data records across funded activities

Data Exchange staff work with organisations to ensure clear information is available to clients to explain what data is captured as part of program performance reporting and used for the purposes of policy development, grants program administration, research, evaluation and provider compliance monitoring processes.

Go to the Data Exchange website and Section 5 of this document for more information about privacy. Program specific guidance on clients, support people and other client level data items is available on the Data Exchange website.

3.2 Who is a client?

For the purposes of recording a 'client' record in the Data Exchange, for CHSP a client is defined as:

> **An individual who receives a service as part of a funded activity that is expected to lead to a measurable outcome.**

3.3 Who is a support person?

At times, there may be other people present at a service who do not meet the definition of a client. This could include carers of clients, family members or children who attend to support the client. Paid employees of an organisation are not counted as support people. The support person is not expected to achieve a direct outcome through this service interaction and is *not* counted as a client.

There are no requirements to record the details of support people in the Data Exchange, however if an organisation wants, they can create an individual record for these people and record them as support people at the session level.

3.4 Services for couples, families and households

The Data Exchange captures information about individual clients, however there are some CHSP activities where multiple individuals are assisted as part of the same 'case', 'family' or 'group'. In these instances, a client record should be created for each individual client and grouped together using a 'case' record.

Table 1. Example of a client and support person

Activity/Service Context	Who is the client?
A couple attends a Social Support Group activity run by the local senior citizen's club. Both persons are eligible to receive services under CHSP.	Both people in the couple are considered clients, as they are both receiving the service, benefit from that service, and meet the definition of a 'client' as per the program activity guidelines. Two client records should be created and used within the Data Exchange.
A person accesses CHSP transport services to attend a doctor's appointment and their carer attends this service as well, so they can assist the person during the appointment.	The person is counted as the client as they have received the service and will achieve an outcome. The carer is not recorded as a client as no measurable outcome is achieved on this occasion. The carer could be recorded as a support person, however this is not mandatory.

3.5 Group session

When delivering CHSP program activities, a group session generally means a session that has three or more clients attending a session together. A group session can be made up of a family group, clients that are known to each other, or strangers. This definition does not count a support person or practitioner as a member of that group.

4 Linking client data to service delivery

4.1 What is a service?

The Data Exchange framework has a specific definition of a service based on service delivery concepts. These concepts ensure that an instance of service is consistently applied across varying funded activities and service delivery contexts that are reported in the Data Exchange. For the purposes of the Data Exchange, a service is defined as:

> **One or more individual instances or episodes of assistance (known as sessions) within a reporting period that are delivered within a distinct case.**

The concept of a 'case' and 'session' are integral to the Data Exchange as they maintain a consistent way for organisations to record information about the different activities clients are accessing, how they are being delivered and the location from which they are being delivered. These concepts are discussed below and in further detail at Section 6 of this document.

Go to the Data Exchange website for program specific guidance for more information on cases and sessions.

4.2 What is a case?

Cases act as containers, linking client and session data to location and program activity information. A case is defined as:

> **A method to capture one or more instances of service (known as sessions) received by a client or group of clients that is expected to lead to a distinct outcome. A case may contain between one and an unlimited number of sessions.**

A case record helps understand what funded activity is being delivered, the location it is being delivered from, the reason clients came to the service and the number of clients receiving a service.

Each organisation can create cases in a format that best suits their needs. However, a case cannot exceed 1000 (one thousand) individual clients.

For users of the web-based portal, cases facilitate navigation and hold clients and sessions together.

- A case can operate over multiple reporting periods, for instance if a client returns to receive the same service.
- Depending on the nature of the service, a case can contain an individual, a couple, a family, or an unrelated group of individuals, such as a regular weekly or monthly group meeting.
- If a client attends a number of different funded activities, each of these is treated as a separate case.
- If a client receives the same services from a number of different locations (known as outlets) managed under the same program activity, each of these is treated as a separate case.
- To report a case, details are recorded about the activity, the location (or outlet) where the service occurred, and the client who will receive the service associated with that case record.

4.3 What is a session?

In the Data Exchange, a session is defined as:

> **An individual instance or episode of service, stored within a case, which is 'related' to other sessions (when/if they occur).**

A session record includes the date the service occurred, the kind of service the client(s) received (known as service type) and which of the clients associated to the case were present. For organisations participating in the partnership approach, client pathways information (referrals out) is recorded at a session level. More information about the extended data set is found in Sections 6 and 7 of this document.

4.4 Counting rules for clients, cases and sessions

A **client** is counted against a reporting period if the client was recorded as attending at least one session within that reporting period.

A **case** is counted against a reporting period if at least one session is recorded under the case within that reporting period.

A **session** is counted against a reporting period if the date of the session fell within the reporting period and at least one client is attached.

4.5 What is an outlet?

For the purposes of the Data Exchange, an outlet is defined as:

> **The physical location from where a service is primarily being delivered.**

- The organisation identifies the program activities each outlet delivers.
- Each outlet can have different staff, service information, program activities, and contact details.
- Where the service is mobile in nature, the outlet used should be the nearest administrative premises where staff are based, and where they are likely to be travelling from to deliver the service.
- Creating multiple outlets for services delivered from the same address must be avoided.
- Post office boxes cannot be used in place of a physical location.
- An outlet should never be created for a client's residential address, if a service is delivered in a client's home, or a sensitive/protected location such as a refuge.
    - In the instance of service delivery at a residential address, the outlet should reflect where staff are based or travelling from. This information is captured with the session details under the service setting field.

- In the instance of service delivery at a protected address or refuge, the outlet can use an address of a non-identifiable public place nearby, such as a post office, police station or shopping centre.

4.6 Delivery partnerships and consortium arrangements

In the Data Exchange, a Delivery Partner is defined as an organisation engaged by the lead organisation (the Grant Recipient) to deliver services to clients on behalf of the lead organisation. Lead organisations make different choices when it comes to setting up their delivery partners and outlets. As these decisions will affect who can enter, view and report data in the Data Exchange, set up needs to happen in agreement between the two parties, e.g. lead/facilitating and delivery partners. Particular attention needs to be paid to the naming of outlets, outlet addresses, the visibility of data and the protection of client privacy and personal information.

Go to the Data Exchange website training resources for guidance on partnerships and consortium arrangements.

5 Protecting a client's personal information

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

Under the Privacy Act, personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

In the Data Exchange, personal information includes the client's name (or pseudonym) and street-level address. For clients of the Commonwealth Home Support Program (CHSP), this also includes their My Aged Care ID (MAC ID).

5.1 CHSP Organisations' Implementation Notice

CHSP-funded organisations are required to capture clients' My Aged Care IDs (MAC ID) against the services delivered. The functionality to record the MAC ID in the Data Exchange will not be available in Stage 1. Organisations will be required to capture this information in their own client management systems until this functionality is available in the Data Exchange.

5.1.1 CHSP-specific Data Exchange privacy protocols

Every user of the Data Exchange is bound by the *Privacy Act 1988* and must ensure they meet these requirements at all times. Data Exchange users must ensure they only access records where a genuine need exists.

There are two components of personal information that are stored in the Data Exchange in relation to CHSP:

- Part 1: mandatory collection of a client's My Aged Care ID
  From 1 July 2025 clients receiving CHSP are required to provide their My Aged Care ID. The MAC ID must be reported to the Data Exchange (when available, see implementation notice at 5.1) and is not subject to client consent as it is required to monitor provider compliance. This is authorised under s 573(1) of the *New Aged Care Act 2024* (NACA)
- Part 2: conditional storage of client name/pseudonym and street-level address in DEX with the client's consent
  Part 2 is only relevant for organisations using the Data Exchange as a client record system for managing the client's case. Organisations seeking to store this information in DEX must obtain client consent to do so.

5.1.2 Mandatory collection of a client's My Aged Care ID

All organisations delivering the Commonwealth Home Support Program must collect and report the My Aged Care IDs (MAC ID) of the clients to whom they are providing CHSP services. The Department of Health, Disability and Ageing uses the MAC ID to assess provider compliance with the statutory funding conditions for home support grant funding (*Aged Care Act 2024* ss 266-267).

Organisations must notify their clients that their MAC ID will be entered into DEX for this purpose. Organisations may choose to incorporate either the mandatory Standard CHSP Privacy Notification or the mandatory components of the CHSP Alternative Privacy Notification.

CHSP-funded organisations who deliver other programs should not enter the My Aged Care IDs of clients who only receive non-CHSP programs.

When organisations enter the MAC ID into DEX, the system will automatically encrypt the ID. The organisation will only be able to see the last three digits of the ID displayed back to them. DSS will only store the full encrypted ID and the unencrypted last 3 digits.

DSS discloses a subset of this information to DoHDA periodically in order to monitor provider compliance with funding grant conditions (compliance purpose). This is authorised under s573(1) of the new *Aged Care Act 2024* (NACA).

DoHDA will decrypt the My Aged Care ID in order to verify information about CHSP services provided to clients for the compliance purpose. DoHDA cannot undertake compliance monitoring activities without this information.

5.1.3 Conditional on consent - storage of client name/pseudonym and street-level address in DEX with the client's consent

Organisations must apply the conditional on consent Data Exchange consent and notification arrangements if they intend to store the non CHSP-specific personal information (client name/pseudonym and street-level address) in the Data Exchange. Where an organisation stores the conditional on consent personal information in the Data Exchange, only the organisation can access the personal information stored on this DSS hosted information system.

The client has the right to decline to have this information stored in DEX. In that case, the organisation will need to ensure they identify the client in their own record system using the DEX Client ID to assign the correct client to their DEX case and session records.

5.1.4 Department of Social Services handling of personal information stored in the Data Exchange

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 use de-identified data from the Data Exchange for program management, policy development, research, and evaluation activities for government. DSS applies best practice data de-identification 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.

Data captured in the Data Exchange will only be used by DSS on behalf of DOHDA for the purpose for which it was captured.

Data Exchange data will not be provided to other parties in Australia or elsewhere in the world for any other purpose.

Go to the Data Exchange website to find out more about the Privacy Impact Assessment conducted by the Australian Government Solicitor which examined the Data Exchange's compliance with the Privacy Act.

5.2 Organisations' obligations when storing personal information in the Data Exchange

Organisations must adhere to the notification and consent requirements identified in this chapter, which ensure that DSS on behalf of DoHDA complies with its obligations under the Privacy Act and the APPs.

To satisfy the notification requirements organisations must include the mandatory – and if applicable conditional on consent - CHSP Standard Privacy Notification (paragraph 5.3.1 below) on their registration forms. If organisations do not wish to use these words on their registration forms, organisations are required to notify the client of the matters outlined in APP 5.2, or ensure that the client is aware of those matters.

In either case, organisations are required to provide the CHSP Standard Privacy Notification (or an alternative notification on privacy) before the time that the client's personal information is entered on the Data Exchange or, if that is not practicable, as soon as practicable after the client's personal information is entered on the Data Exchange.

5.2.1 CHSP Standard Privacy Notification

Drafters notes and explanatory text in red should be removed prior to the notification being included in Organisations' registration forms.

Mandatory:

The following 'CHSP Standard Privacy Notification', up until 'Conditional on consent' (unless using the CHSP Alternative Notification for Mandatory elements) **must** be included in Organisations' registration forms used for CHSP services.

The Mandatory standard notification is outlined below:

"Collection of your My Aged Care ID

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 Department of Health, Disability and Ageing (DoHDA) provide grant funding to providers of aged care services under the Commonwealth Home Support Program (CHSP).

CHSP providers must report on the delivery of CHSP services to DoHDA via the Data Exchange (DEX).

This system is hosted by the Australian Government Department of Social Services (DSS).

DSS on behalf of DoHDA collects information (including information about the services you receive and an encrypted version of your 'My Aged Care ID') from your CHSP provider and stores this information as a de-identified record in DEX. This protected information is a mandatory requirement and is not used by DSS for any purpose.

Uses and disclosures of your My Aged Care ID in the Data Exchange

DSS on behalf of DoHDA discloses a subset of this information (including an encrypted MAC ID) to DoHDA periodically in order to monitor provider compliance with funding grant conditions (the compliance purpose). This is authorised under s 573(1) of the *New Aged Care Act 2024* (NACA).

DoHDA will decrypt your My Aged Care ID in order to reidentify you and verify information about CHSP services provided to you for the compliance purpose. DoHDA cannot undertake compliance monitoring activities without this information.

How DSS uses and discloses personal information other than My Aged Care ID in the Data Exchange

DSS on behalf of DoHDA uses your information in DEX to produce and share de-identified data and data visualisation reporting products to DoHDA and providers, for reporting and research purposes.

DSS uses your information in the Data Exchange to produce information for policy development, grants program administration, and research and evaluation purposes. DSS also shares data with organisations and agencies for reporting and research purposes. DSS de-identifies all data before use or disclosure so that it cannot be used to re-identify you.

Further information

For more information about how DSS on behalf of DoHDA will manage your personal information, including how you can request access or correction of your personal information or make a privacy complaint, see the privacy policy published on the DSS website."

Conditional on consent:

In addition to the above which must always be provided to CHSP clients, Organisations using the Data Exchange as a client records system must include the 'Conditional on consent - CHSP Standard Privacy Notification' on their registration forms. This is to enable DSS to store a client's personal information (other than the My Aged Care ID) on the Data Exchange.

The Conditional on consent standard notification is outlined below:

"**Our use of the Data Exchange**

We are also using the Data Exchange as a client record system. Your personal information (other than your My Aged Care ID) that is stored by DSS on the Data Exchange will only be disclosed to us for the purposes of managing your case.

DSS will only collect certain personal information with your consent

Your client record can be set up to include your name and address. This assists us to manage your record but will require DSS to collect personal information about you.

You are not required to provide your name and address to DSS. If you do not consent to the collection of your personal information, this will not affect the services provided to you. You can ask for this information to be removed by DSS at any time."

5.2.2 CHSP Alternative Privacy Notification

If organisations do not wish to include the CHSP Standard Privacy Notification on their registration forms, they may design and use their own forms to collect and store the mandatory, and where relevant conditional on consent, personal information in the Data Exchange. If organisations wish to follow this approach, they are required to notify the client or otherwise ensure that the client is aware of the following matters (as outlined in APP 5.2):

Mandatory: these elements must be included for all CHSP clients, in relation to the collection and reporting of their My Aged Care ID.

(a) The Department of Health, Disability and Ageing (DoHDA) provide grant funding to providers of aged care services under the Commonwealth Home Support Program (CHSP).

(b) CHSP providers must report on the delivery of CHSP services to DoHDA via the Data Exchange (DEX).

(c) the Data Exchange is an IT system that is hosted by DSS.

(d) DSS on behalf of DoHDA collects information (including information about the services received and an encrypted version of a client's 'My Aged Care ID') from you and stores this information as a de-identified record in the Data Exchange.

(e) With the exception of My Aged Care ID, 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

(f) 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

Conditional on consent:

In addition to the above elements, the organisation must notify the client of the following conditional on consent elements if they are using the Data Exchange as a client record system i.e. intending to store the client's name/pseudonym and street level address on DEX.

(g) the organisation is using the Data Exchange for recording client information, and the client's personal information (with the exception of the encrypted version of the My Aged Care ID) is stored on the Data Exchange for this purpose only.

(h) 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

(i) the consequences if personal information is not collected from the client.

This notification is necessary to enable the client's personal information to be stored on the Data Exchange by DSS in compliance with the Privacy Act. DSS will not review, approve or store an organisation's registration forms.

5.2.3 Consent to collect and store conditional on consent personal information

Before submitting a client's name (or pseudonym) and street-level address to the Data Exchange, in addition to providing the required notification to a client, an organisation will need to:

- obtain the express consent of a client, for DSS on behalf of DoHDA to collect the client's personal information from the organisation and store it on the Data Exchange
- record that consent in the Data Exchange IT system
- inform the client that they may withdraw this consent at any time.

DSS on behalf of DoHDA will not store the client's name or pseudonym, and/or street-level address on the Data Exchange unless this consent is obtained.

To meet DSS's obligations under the Privacy Act, the required consent is to be recorded in the Data Exchange. For organisations using the web-based portal, consent is recorded using the tick box provided when creating or editing a client. When reporting client-level records through bulk uploading of files or a system-to-system transfer, this consent is to be recorded in these files.

Consent must be given openly and obviously, either verbally or in writing. Organisations are required to record that a client has consented in the Data Exchange, however they are not required to provide copies of the client's consent to DSS. Organisations should determine their own record keeping procedures in relation to client consent.

If a client withdraws consent for DSS on behalf of DoHDA to store their personal information on the Data Exchange, an organisation must record the client's decision in the Data Exchange. Organisations using the web-based portal will need to 'un-tick' the consent for personal information box. Organisations that report

using system-to-system transfers or bulk uploads will need to update the client level record in the Data Exchange consistent with a client's decision to withdraw their consent.

When an organisation has recorded a client's decision in the Data Exchange, DSS will process the withdrawal of consent by removing the record of the client's name or pseudonym, and/or street-level address from the Data Exchange.

5.3 Obtaining consent from individuals with compromised capacity

When obtaining consent from a client whose capacity to consent may be compromised (e.g. a client with a physical or mental disability), it might be appropriate to implement special practices. For example, the organisation should consider who can provide consent on the client's behalf. Options include a guardian, someone with an enduring power of attorney, a person recognised by other relevant laws (e.g. a 'person responsible' under the Guardianship Act 1987 (NSW)) or a person nominated in writing by the client while they were capable of giving consent.

5.4 Consent for follow up research

Funding agencies and third parties (such as universities) are interested in commissioning future research to better understand client needs and find opportunities to improve service delivery. Obtaining client consent to participate in research will create an indicative pool of willing participants for future research projects.

Organisations must ask clients if they consent to participate in future client research. This consent forms part of the priority requirements. Future research will vary depending on the nature of the planned evaluation; however, the basic steps are:

- Any research conducted will be approved by a recognised ethics committee.
- Researchers will communicate with organisations before any research activities start.
- Organisations and researchers commit to clear and simple communications to help clients understand why research is important and what it means to participate.
- Clients can withdraw their consent at any time.

5.5 Organisational privacy considerations

Once a client record is created, it is visible to all Data Exchange users within the organisation. Organisations must address any potential privacy issues through their own internal business processes.

Organisations should never provide a client's personal information to DSS via telephone or email communications, for example when contacting the Data Exchange Helpdesk.

5.6 De-identified data

The Data Exchange protects client privacy by applying best practice data de-identification and aggregation methods, including the use of statistical linkage keys for data matching.

5.6.1 Unique client identifiers

A unique client identifier is used to ensure client records are matched in the Data Exchange.

Two data items (date of birth and gender) are included in the priority requirements to help identify individual clients without disclosing personal information. Program performance data provided by organisations through the Data Exchange is de-identified and encrypted so that no personal client information is accessed by DSS or any other agency.

5.6.2 DSS Statistical Linkage Key (SLK)

The Data Exchange de-identifies client data using the DSS Statistical Linkage Key (SLK). The DSS SLK is a method that allows DSS to link clients with the service they received through a unique key, enabling two or more records belonging to the same individual to be linked – regardless of which service they received and from where.

The SLK is an algorithm that creates a code consisting of the second, third and fifth characters of a person's family name, the second and third letters of the person's given name, the day, month and year of the person's date of birth and the self-identified gender of that person. For example, John Smith, a male born on 14th February 1971 has a DSS SLK of: **MIHOH140219711**

A client's DSS SLK is not visible to organisations in the Data Exchange. The DSS SLK is only visible to a highly restricted number of DSS employees who perform database administration or data analytics duties to ensure the IT system behind the Data Exchange remains functional and to support data sharing and reporting initiatives.

For organisations using the Data Exchange web-based portal, the DSS SLK is automatically generated within the system. For organisations using bulk uploads or system-to-system transfers to upload data to the Data Exchange, the DSS SLK can be incorporated into their own client management information system using the above algorithm. This DSS SLK must not include shortened versions of a client's name, nickname or any variations of their full name, or any other information that could identify a client.

Go to Data Exchange website for help configuring systems to push the DSS SLK across to the Data Exchange.

5.6.3 Client ID

Each client record in the Data Exchange includes a client ID that must remain unique to that client in all circumstances while connected to the funded organisation. This is different to the DSS SLK described above.

The client ID is made up of a series of alphanumeric text, either inputted by the organisation or created by the Data Exchange web-based portal, specifically.

Web-based portal

- Organisations have the option of entering their own client ID (an ID used internally by the organisation), which must **not** include any information that could identify the client, or
- leave the field blank, where the portal will generate a client ID that is used by organisations to search for their record later.

Where an organisation chooses to enter their own client ID, this should be alphanumeric or numeric text only. This Client ID must not include shortened versions of a client's name, nickname or any variations of their full name, or any other information that could identify a client, under any circumstances.

Bulk upload or system-to-system transfer

- For organisations using their own client management system and uploading their data to the Data Exchange, the client ID becomes a mandatory field from their own system and used to cross-reference the record between the two systems in future interactions.

Go to the Data Exchange website for technical specifications.

5.7 Identified data

A unique client identifier; My Aged Care ID, is a mandatory requirement for CHSP providers to capture, to allow DoHDA to reidentify individual clients and verify information about CHSP services provided to monitor provider compliance.

On behalf of DoHDA, the Data Exchange only collects individual clients' protected information (an encrypted version of a clients' 'My Aged Care ID'). This protected information is stored as a de-identified record in the Data Exchange and is not used by DSS for any purpose.

DSS on behalf of DoHDA discloses a subset of this information to DoHDA periodically in order to monitor provider compliance with funding grant conditions (compliance purpose). This is authorised under s 573(1) of the *New Aged Care Act 2024* (NACA).

DoHDA will decrypt individual clients' aged care ID in order to reidentify clients and verify information about CHSP services provided to them for compliance requirements. DoHDA cannot undertake compliance monitoring activities without this information.

The decryption of individual clients' My Aged Care ID does not occur within the Data Exchange.

Refer to 5.2.1 for 'CHSP Organisations' Implementation Notice'.

5.8 Cyber Security Incidents and Data Breaches

Organisations are responsible for implementing processes and controls to protect Data Exchange information from unauthorised access.

Organisations must notify the DoHDA as soon as practical if they become aware of an actual (or possible) cyber security incident and/or data breach.

5.8.1 Cyber Security Incidents

According to the Australian Cyber Security Centre's (ACSC) Guidelines for Cyber Security Incidents, a Cyber Security incident is:

> *A cyber security incident is an unwanted or unexpected cyber security event, or a series of such events, that either has compromised business operations or has a significant probability of compromising business operations.*

For the purposes of the protocols, unauthorised access to the Data Exchange system is a cyber security incident.

Organisations must have processes and controls in place to prevent and manage cyber security incidents for the Data Exchange. For example, ACSC's Small Business Cyber Security Guide recommends organisations:

- make an **emergency plan**, including processes for staff to report potential cyber security incidents
- **educate employees** on cyber security issues, including:
    - encouraging employees to visit cyber.gov.au/learn
    - adding cyber security training or practices into the induction process
    - encouraging positive security habits in staff
- implement Data Exchange **access controls**, including ensuring:
    - users have only the minimum permissions required to perform their work
    - revoking access for staff who leave the business.

All users with access to DSS IT resources have particular responsibilities in respect of:

- Password security. No-one is to attempt to bypass or defeat DSS' IT security system.
- Everyone is responsible for maintaining the integrity of software and hardware under their ownership and ensuring that its condition does not prejudice the integrity of DSS' propriety or licensed software or hardware.

The following resources may assist organisations in meeting their Data Exchange cyber security responsibilities:

- ACSC's Resources for business and government at https://www.cyber.gov.au/.
- Australian Charities and not for Profit Commission's (ACNC) Governance Toolkit: Cyber Security at https://www.acnc.gov.au/

5.8.2 Data Breaches

According to the Office of the Australian Information Commissioner (OAIC):

> *A data breach happens when personal information is accessed, disclosed without authorisation, or is lost*

Should a client's **personal information** in the Data Exchange be shared with or accessed by an unauthorised person, this constitutes a **data breach** under the *Privacy Act 1988*. A data breach may occur as part of a cyber security incident.

Organisations should have processes and controls in place to prevent and manage data breaches for the Data Exchange. For example, Office of the Australian Information Commissioner's (OAIC) Protecting customers' personal information recommends organisations:

- have personal information handing processes and procedures, and ensure staff undertake regular privacy training
- ensure staff access personal information on a need-to-know basis
- have policies on information security, including ICT security, physical security and access security take care when handling sensitive information
- have a data breach response plan.

The following OAIC resources at https://www.oaic.gov.au/privacy/ may assist organisations in meeting their Data Exchange privacy and data breach responsibilities:

- Privacy guidance for organisations and government agencies
- Data breach preparation and response guide.

6 Collecting the priority requirements

The priority requirements are a small set of mandatory data items. These data items capture the demographics of clients accessing program activities, how often clients are attending, where they are attending and what program activities they are attending.

In summary, the priority requirements reflect the collection of information about client details, case and session details, and client consent to participate in follow-up research.

This section presents practical information about each of these concepts to support managers and frontline staff to consistently and accurately collect the required data.

Go to the Data Exchange website for more information on configuring systems and service delivery information such as how to use cases, sessions and service types. The data values are listed in Section 11 of this document.

6.1 Client level data

Client-level priority requirements capture client details and demographic characteristics. This provides an understanding of each client's pathways over time, on a de-identified basis.

A client record only needs to be created once. It can then be maintained, updated and edited at any time.

Client level data is reported for all individuals who receive a service as part of a funded activity, in line with the definition outlined in Section 2 and 3 of this document. These records are the basic 'building blocks' of the Data Exchange Framework and are used to answer standard questions such as:

- how many clients were assisted?
- how many clients were assisted in previous reporting periods?
- how many clients received assistance under different funded activities?
- how many clients received assistance from a funded activity delivered by a different organisation?
- how many clients receiving assistance were from vulnerable target population groups?

Answers to these questions will help tell the broader story about the outcomes being achieved, by providing an understanding of **who** these outcomes are being achieved for and **when**.

6.1.1 Collecting client given and family names

Collecting a client's name would typically occur the first time that a client accesses any funded activity from an organisation, either in a registration form or in an intake interview. Organisations are free to gather this information in accordance with their standard practices.

A client's given name and family name are recorded because they form part of the SLK used to uniquely identify clients without disclosing personal information. **Given name** is typically a client's first name, but it may include one or more middle names. Ideally, the given name should be recorded exactly as it is on key identification documents such as a passport or driver's license.

Family name is typically the client's last name, or surname, and ideally should be recorded exactly as it is spelled on key identification documents.

Where clients are known by more than one name, or prefer to be called by a particular name, for example Joe rather than Joseph, their given and family names should reflect the name the client offers.

6.1.2 Date of birth

A client's date of birth is recorded for two reasons: it forms part of the SLK and provides a direct means of calculating the client's age.

Age groups demonstrate part of the standard demographic profile for clients required by many government programs and is of particular importance to programs that target age-specific cohorts.

Where a client does not know their date of birth or does not wish to disclose it, it is acceptable for an estimated date of birth to be used. An estimated date of birth indicator is in the Data Exchange and should be used to flag when this occurs. For example, if a client thinks they are approximately 70 years old (and it is 2025), the estimated date of birth indicator is flagged, and the year of birth is recorded as 1955.

6.1.3 Gender

A client's gender is recorded because it forms part of the SLK and is recorded based upon how the client self-identifies. Please note that gender is different to sexuality and sexual orientation, which are not recorded in the Data Exchange.

The Data Exchange uses standard data definitions for gender developed by the Australian Bureau of Statistics (ABS) under their new Standard for Sex, Gender, Variations of Sex Characteristics and Sexual Orientation Variables, 2020, with five options::

- Man or Male
- Woman or Female
- Non-binary
- Different term [Free text field up to 100 characters]
- Prefer not to answer

The ‘Non-binary’ response is used where a client does not identify as male or female. Should a client use a term that does not align with the term listed, the term can be described under ‘Different term’. If a client chooses not to disclose their gender, it is acceptable to record ‘Prefer not to answer’.

6.1.4 Residential address

Information about where clients live can assist with understanding if services are located in the right area.

A client’s residential address can also be compared to an outlet address to understand how far the client may be travelling to access a service, or how far staff may be travelling to deliver a service to a client.

A client’s residential address can also be linked to other useful information to help understand a client’s circumstances, such as the Socio-Economic Indexes for Areas (SEIFA) rankings and the Australian Bureau of Statistics (ABS) community profiles.

Within the Data Exchange, there is the capacity to record a full residential address for each client. At a minimum, a client’s state, suburb and postcode are considered part of the priority requirements and must be recorded to create the client record.

The identity of clients providing their full residential address is protected by converting the data to the Australian Statistical Geography Standard. This means that a geography code is recorded in place of the client’s address, which de-identifies the record.

In exceptional circumstances, it may not be appropriate to record the client’s full residential address, such as where the client is experiencing domestic violence and does not wish to provide even their suburb, state and postcode due to fears for their personal safety. In these circumstances, the service outlet suburb, state and postcode should be recorded instead.

6.1.5 Recording a homeless client’s residential address

If a client is homeless or of no fixed address, the client or organisation can determine the most appropriate address to be recorded. This may be the suburb, state and postcode of where the client usually spends the night, or suburb, state and postcode of the outlet where the client is seeking assistance. A flag to indicate the client is currently homeless is in the extended demographics section of the Data Exchange.

6.1.6 Indigenous status

A client’s Indigenous status is recorded to provide an important understanding of whether clients who identify as Aboriginal or Torres Strait Islander origin are accessing services. Under standard data collection definitions used by the AIHW, five options are available to record a client’s Indigenous status.

Indigenous status is part of the standard demographic profile for clients of many government programs and is of particular importance in ensuring Indigenous people and communities have appropriate access to funded services.

Where a client chooses not to disclose their Indigenous status, it is acceptable to record ‘Not stated/Inadequately described’.

6.1.7 Cultural and Linguistic Diversity (CALD)

A client’s CALD background is recorded to provide an important understanding of whether CALD clients are accessing services. Under standard data collection definitions used by the Australian Institute of Health and Welfare (AIHW), two questions are used to record a client’s CALD status:

(a) Country of birth

- Record the country of birth indicated by the client
- A list of values is based on the Australian Bureau of Statistics Standard Australian Classification of Countries (SACC), 2016

(b) Main language spoken at home

- Record the main language spoken at home indicated by the client.
- A list of values is based on the Australian Bureau of Statistics Australian Standard Classification of Languages (ASCL), 2016

More detailed information about a client's CALD background such as ancestry is collected in the extended demographics section of the Data Exchange.

CALD status is part of the standard demographic profile for clients of many government programs and is of particular importance to ensure CALD clients and communities have appropriate access to funded services.

This information can also be beneficial for organisations in determining whether the engagement of translating services or bilingual staff may assist in better service delivery for their clients. Where a client chooses not to disclose their CALD status, it is acceptable to record
'Not stated/Inadequately described'.

6.1.8 Disability, impairment or condition

Clients are asked to self-identify whether they have a disability, impairment or condition because it is important for organisations and funding agencies to know whether clients with disability are accessing services.

Under standard data collection definitions used by the AIHW, disability is recorded in groupings that most clearly express the experience of disability by a person. Disability groupings constitute a broad categorisation of disabilities in terms of the underlying health condition, impairment, activity limitations, participation restrictions, environmental factors and support needs. Categories in the Data Exchange include:

- **Intellectual/learning**: associated with impairment of intellectual functions which limit a range of daily activities and restrict participation in a range of life areas, for example, but not limited to; dyscalculia, dysgraphia, dyslexia.
- **Psychiatric**: associated with clinically recognisable symptoms and behaviour patterns frequently associated with distress that may impair personal functioning in normal social activity, for example, but not limited to; Asperger syndrome, attention deficit hyperactivity disorder, autism, behavioural disorders, bipolar, depression, eating disorders, epilepsy, manias, phobias, schizophrenia, somnias.
- **Sensory/speech**: including vision disability (blindness, vision impairment); hearing disability (deafness, hearing impairment that cause severe restrictions in communication); deaf-blind (dual sensory impairments causing severe restrictions in communication); speech disability (speech loss, impairment which causes severe restrictions in communication).
- **Physical/diverse**: associated with the presence of an impairment, which may have diverse effects within and among individuals, including effects on physical activities such as mobility. This grouping includes physical disability, for example; paraplegia, quadriplegia, muscular dystrophy, motor neurone disease, neuromuscular disorders, cerebral palsy, absence or deformities of limbs, acquired brain injury, neurological disability (including epilepsy, dementias, multiple sclerosis and Parkinson disease).
- **None**: no disability, or no disability, impairment or condition are identified by the client.
- **Not stated/inadequately described**.

When recording data about disability, impairments or conditions clients should self-identify, and can identify with more than one group, for example physical/diverse and intellectual/learning.

Data about disability status is part of the standard demographic profile for clients of many government programs and is of particular importance to ensure people with a disability have appropriate access to funded services. Where a client chooses not to disclose if they have a disability, impairment or condition, it is acceptable to record 'Not stated/Inadequately described'.

6.2 Service delivery information

The concept of a case and session are integral to the Data Exchange as they maintain a consistent way to link a client with instances of service and to help tell the 'story' about outcomes achieved for clients.

Once a client record is created in the Data Exchange, it must be linked to the program and activities the client is participating in. This is captured using the case and session records. A case is the first step in recording service delivery information within the Data Exchange.

6.2.1 Case details

The second tier of the priority requirements is a case record, which includes a case ID, program activity, and outlet information. A case record is only created once for each unique case and is used over multiple reporting periods.

Each case record includes:

- **Case ID**: an alphanumeric code or title that uniquely identifies the case, and which is named in a way that is meaningful to the user. The case ID business rules are the same as those for the client ID: the case ID must be unique within the organisation and not include any identifiable information, such as a client's name or their Centrelink Customer Reference Number. Users of the Data Exchange web-based portal may leave the field blank, in which a case ID is automatically generated (numeric only). The field is mandatory for those uploading data through the bulk upload or system-to-system methods.
- **Program activity**: the funded activity that the case is being delivered under.
- **Outlet**: the location where the case is primarily being delivered. A case cannot have more than one outlet.
- **One or more client records**: links one or more clients to a case (or in limited circumstances an aggregate number of unidentified clients).

The number of case records an organisation creates will depend on the type of funded activity(ies) they deliver and the way these services are delivered. For example, if providing counselling to couples or families it would make sense to create a case for each couple/family. This would allow a user to see and reflect on the family composition of each couple/family, easily navigate the portal for efficient data entry, and potentially count the total number of cases as the number of couples/families accessing services.

In contrast, for organisations delivering activity-based services, it may be better suited to create a case for each of the locally run activities delivered in the community, such as a breakfast club or education course.

For organisations using the bulk upload or system-to-system method, the concept of a case is a node that allows all three tiers of the Data Exchange data (clients, cases and sessions) to be effectively uploaded.

6.2.2 Session details

The third tier of the priority requirements is a session record. A session record captures the types of services being delivered under the relevant case, which clients attended, and the dates of service. Sessions also indicate that a case was active within a reporting period. Each session record consists of:

- **Session ID**: a numeric code or title that identifies a particular instance/ episode of service. The session ID must be unique within the case and cannot include identifiable client information. Users of the Data Exchange web-based portal may leave the field blank, and a session ID is automatically generated (numeric only). The field is mandatory for those uploading data through the bulk upload or system-to-system methods.
- **Session date**: the date the instance/episode of service occurred.
- **Service type**: the main focus for the session delivered. If a session covered multiple service types the most relevant one should be chosen, either based on the majority of time spent or the main way an outcome was achieved.

- **Client attendance**: recorded for each client that was present at the session.
- **Unidentified client attendance**: the aggregate number of unidentified clients who attended a session. This should be limited to large groups where the collection of client level information is not feasible. Unidentified client attendance at a session must be less than or equal to the number of unidentified clients against the case.

When recording a session, organisations should select the service type, which best reflects the nature of service delivery in that particular session. Different service types are associated with different funded activities. Within the Data Exchange web based portal, only the relevant service types are available for a user to choose.

For organisations using the bulk upload or system-to-system method, sessions are a node that complete all three tiers of Data Exchange data (clients, cases and sessions) being effectively uploaded.

6.3 Program specific mandatory fields

The Data Exchange Framework establishes streamlined and standardised program performance reporting to inform priority requirements. A small number of funded activities require additional mandatory data items to be reported. Go to Section 11 of this document for a comprehensive list of the field values.

6.3.1 Commonwealth Home Support Programme mandatory fields

The following items are required and will only present if the client is participating in the Commonwealth Home Support Programme activity:

- **Accommodation setting**: organisations are asked to record the accommodation setting category that best describes that of the client.
- **Living arrangements**: this is required for this program activity as it provides important information about a client's presenting context. Living arrangements and its categories are adapted from the data collection definitions used by the AIHW. This information can also be collected as 'household composition' in the partnership approach.
- **DVA card status**: a client's Department of Veterans' Affairs (DVA) card status is collected.
- **Existence of a Carer**: this field is required to determine how many clients have care arrangements in place. This question is a yes/no response.
- **Amount of assistance provided**: measured as hours and minutes, quantity, cost and/or type. These data fields will only present once the service type is selected in the session. For more information go to the program specific guidance on the Data Exchange website.
- **Fees charged**: this item is captured at the session level. It allows organisations to report whether the participants of the session were charged a fee to attend the service and reflects the program activity policy regarding fee collection. This item is captured as a dollar figure.
- **Exit reason**: users can record the reason a client exited a service. See section 7.1 for list of available exit reasons.

7 Collecting partnership approach data

The Partnership Approach is a collection of extended data items as well as Standard Client/Community Outcomes Reporting (SCORE) data items.

DoHDA does not require CHSP providers to collect SCORE, however selecting an Exit reason at the case level is a requirement. Exit reason forms part of the extended data set.

If a CHSP provider opts to collect any other Partnership Approach data, they need to refer to the Data Exchange Protocols document for relevant information.

DoHDA requires their organisation to select an exit reason

7.1 Exit Reason

This data provides information about the circumstances surrounding the ending of a client's relationship with a case. This contributes to a general understanding of the patterns of client interaction with a program and gives indications as to reason a client might disengage with a service. The Exit Reason categories in the Data Exchange are:

- **Client no longer requires assistance**: the client is now able to manage without any formal assistance. For example, if the client is managing on their own, or with the help of family or friends, or if they only needed temporary assistance. This may be used where a client's circumstances have improved to the point that they no longer require assistance, but not necessarily because the service met their needs.
- **Service unable to provide assistance**: the organisation has ceased delivering services to the client because of the organisation's resource limitations, or because the organisation no longer considers it safe or appropriate for staff or volunteers to continue to assist the client.
- **Client now requires higher level of care**: the client's increasing dependency or need for assistance has reached the point where the organisation can no longer provide the necessary assistance, and the client is referred to a more appropriate source of care.
- **Client has moved out of area**: the organisation is no longer able to assist the client because their residential location has changed and is out of the geographic area of coverage of the organisation.
- **Client terminated the service**: the client chose to cease services or refuse further assistance from the organisation.
- **Client died.**
- **Client no longer eligible**: the client no longer meets the eligibility criteria of the program to receive the service. For example, a program's eligibility might be for children aged 6 – 16, and once the client has turned 17, they are no longer eligible for the service.
- **Client needs have been met**: the client no longer needs assistance from the organisation because their circumstances have improved as a result of the reason they sought assistance and the service they received.
- **None of the above**: the circumstances do not reasonably fit any of the above.

8 Data Exchange reports

As part of the Data Exchange, all organisations that use the Data Exchange will have access to their own set of reports, which reflect the information submitted by their organisation. All available reports are accessed via the Data Exchange web-based portal. The ability to access the data and run reports will reflect the level of user access within the organisation.

Go to the Data Exchange website for detailed information on this topic and access to related information.

8.1 Report types

Standard self-service reports

These reports cover the mandatory priority data submitted by the organisation during a particular reporting period. For a current open reporting period the report will refresh every 24 hours to allow near real-time access to the information transmitted.

Partnership approach reports

Organisations participating in the partnership approach have access to a sophisticated suite of additional reports. Using both priority requirement data and extended partnership data, combined with government and population data sets, these reports provide valuable insights into service delivery and client outcomes.

8.2 Benefits of reports

Reports make the data entered visible and enables verification of data quality and integrity. They also provide organisations with an evidence base for evaluation and to inform best practice. The Data Exchange uses de-identified, aggregate information to look at both short- and long-term outcomes achieved for clients across the broad suite of in-scope programs. The reports allow for an understanding of the collective impact of service provided and what combinations of services deliver the best outcomes for clients.

8.3 Access and visibility of reports

Within the Data Exchange, access and visibility of reports will depend on the way organisations set up their outlets and delivery partners.

By default, organisations cannot see a delivery partner's data. However, the 'handshake' allows the sharing of reports data in the form of de-identified, aggregate information. The handshake is a virtual agreement between a lead organisation and their delivery partner(s), to share data from the delivery partner to the lead organisation for their activity. Under a handshake, a lead organisation can only access data reported by the delivery partner for the agreed program(s).

9 Administrative matters

9.1 Access and set-up

In order to use the Data Exchange, an organisation must complete a number of access and set-up steps before client and session information is entered into the system. Organisations are strongly encouraged to complete these steps as early as possible in the reporting period.

They include:

- applying for Digital Identity online
- submitting a User Access Request to the Data Exchange Helpdesk
- accessing the Data Exchange web-based portal to set up their organisation
- create Outlets
- add program activities to Outlets
- add delivery partner details (if required)
- create additional users (if required)
- setting up bulk uploads (if required).

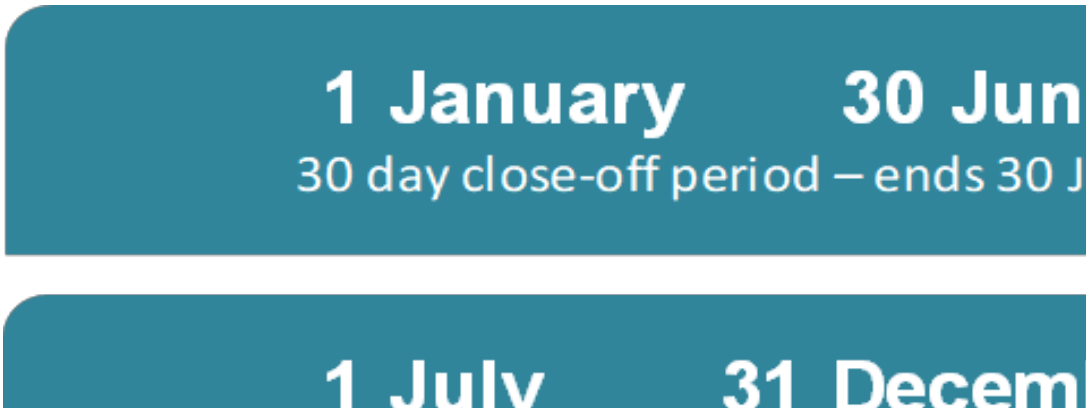
Go to the 'Quick Start Guide' on the Data Exchange website.

Completing access and set-up steps in a timely manner is the responsibility of the organisation as part of their funding agreement obligations.

If these steps are completed too close to the end of a reporting period, the department may not be able to process access and set-up requests with sufficient time remaining for the organisation to complete their data reporting before the due date.

9.2 Reporting periods and deadlines

The Data Exchange has two standardised six-monthly performance reporting periods each year:



Users of the Data Exchange have an extra 30 days at the end of each reporting period, known as the 'close-off period', to allow time to quality check their data and make amendments to reported data. After the 30-day close-off period the Data Exchange automatically closes and no longer accepts uploads for that reporting period.

Organisations can enter data at any time within a reporting period, and are encouraged to do so regularly to make best use of the self-service reports and avoid unnecessary backlog or 'crunch' periods. Organisations new to the Data Exchange, in particular, need to plan for and allow sufficient time for access, set-up and other lead times, in order to meet reporting deadlines.

Once a reporting period has closed, data relating to that period of time will no longer be able to be recorded. Data outside of a reporting period may only be entered if an organisation has sought and is granted a system re-opening.

9.3 Compliance issues and system re-open requests

If an organisation experiences a crisis or event outside of their control that will impact their ability to meet performance reporting requirements, they can request a re-opening of the system.

System re-opening requests are submitted via the 'Request to re-open the Data Exchange form' on the Data Exchange website, however organisations should also consult with their Funding Arrangement Manager or funding agency contact.

System re-openings will only be granted under exceptional circumstances following consultation with Funding Arrangement Managers. Submission of a request does not guarantee a system re-opening will be granted.

9.4 Flexible ways to transmit data

Users can transmit their data to the Data Exchange in one of three ways; system-to-system transfer, bulk file upload, or manual entry into the web-based portal. It is recommended to select one of these as the main transmission method for the longer term. However, in some circumstances, such as the period of initial transition into the Data Exchange, manual entry may need to be used in combination with another transmission method.

All users of the Data Exchange must have a Digital Identity before registering for the system. Digital Identity is a safe, secure and convenient way for Australians to prove who they are online. You can also link your Digital Identity to an Australian business to act on its behalf. Digital Identity allows you to verify your identity, much like a digital version of a 100-point ID check.

Once set up your Digital Identity, you can reuse it whenever you are asked to prove who you are to access a range of government online services for both personal and business matters. More information about Digital Identity can be found here.

At least one person within each organisation will need to complete and submit the Data Exchange User Access Request Form to have Org Administrator access to the Data Exchange. We recommend multiple employees of each organisation hold a Digital Identity. The User Access form is on the Data Exchange website.

9.4.1 System-to-system transfers

Organisations with their own client management software systems capable of pushing data via web services through to the Data Exchange can continue using this software to collect and transfer their performance data. Organisations will need to make a one-off adjustment (or 'enhancement') to their application in accordance with the Data Exchange Web Service technical specifications. The technical specifications are updated periodically to reflect enhancements to the Data Exchange system and are on the Data Exchange website.

9.4.2 Bulk File Upload

Organisations with their own client management software systems capable of creating and exporting XML files can continue using this software to collect and transfer their performance data. Organisations will need to make a one-off adjustment (or 'enhancement') to their application in accordance with the Data Exchange bulk upload technical specifications. The technical specifications are updated periodically to reflect enhancements to the Data Exchange system and are on the Data Exchange website.

9.4.3 Free web-based portal

Organisations can use the Data Exchange web-based portal to manually input their data. Once saved in the portal, data is automatically submitted to the Data Exchange. The web-based portal can be used to directly input client data that is relevant to performance reporting. This option is available for organisations who do not have a system or whose systems cannot accommodate the requirements to submit data through system-to-system transfers or bulk file upload

The Data Exchange web-based portal collects the data requirements set out in this document and is available to all organisations funded to deliver in-scope program activities.

Organisations that already have their own case/client management system and submit their data by system-to-system transfers or bulk upload can access the web-based portal to use the Data Exchange functionality. For example, organisations who report information (consistent with the priority requirements) via a system-to-system transfer or bulk upload, may also use the web-based portal to record SCORE information about changes to their client's circumstances, goals and outcomes (consistent with the extended data items in the partnership approach). This approach is useful where the functionality for recording and reporting the extended data items is not available within an organisation's existing client management system.

Organisations who choose to report using both their client management systems (i.e. via a system-to-system transfer or bulk upload) and the web-based portal are able to view the records of their clients from the web-based portal to monitor and manage the services they provide to these clients.

9.5 Organisations no longer reporting via the Data Exchange

Organisations that report performance data in the Data Exchange are able to receive self-service reports on the data submitted for that period. They will not be able to enter any additional data for a period that has closed or for any periods where they do not have an active funding agreement.

If an organisation is continuing to report on other active activities in the Data Exchange they will have access to Data Exchange reports for all activities they are funded to deliver. Organisations retain access to the Data Exchange portal and self-service reports for at least one full reporting period (six months) after their last activity has ceased.

9.6 Training materials and help

Users of the Data Exchange web-based portal can access self-guided training material on the Data Exchange website.

Task cards

Task cards take users step-by-step through the processes required to create and manage records in the Data Exchange web-based portal.

e-Learning modules

Users of the Data Exchange can also access a suite of training videos known as e-Learning modules. These videos are on the Data Exchange website.

The Data Exchange Helpdesk

The Helpdesk is available to provide technical help to users of the Data Exchange.

You can contact the Data Exchange Helpdesk by email to dssdataexchange.helpdesk@dss.gov.au or on 1800 020 283.

10 List of data values

Table 2. Priority requirements: client level data

Data Field	Protocols Section	Field Values
Client ID	5.6.3	Free text limit of 50 characters. If left blank a system generated number is assigned in the web-based portal, beginning at 001.
Given name *	6.1.1	Free text limit of 30 characters
Family name *	6.1.1	Free text limit of 30 characters
Date of birth *	6.1.2	Date format of dd/mm/yyyy
Estimated date of birth *	6.1.2	Tick box
Pseudonym used	6.1.1	Tick box
Gender *	6.1.3	Man or male Woman or female Non-binary [I/They] use a different term (please specify) Not stated
Residential address	6.1.4	Residential address line 1 (optional) Address line 2 (optional) Suburb (mandatory) State (mandatory) Post code (limit of 4 digits) (mandatory)
Indigenous status	6.1.6	No Aboriginal Torres Strait Islander Aboriginal and Torres Strait Islander Not stated/inadequately described
Cultural and Linguistic Diversity: Country of Birth	6.1.7	Drop-down list of values based on the Australian Bureau of Statistics Standard Australian Classification of Countries (SACC), 2016
Cultural and Linguistic Diversity: Main language spoken at home	6.1.7	Drop-down list of values based on the Australian Bureau of Statistics Australian Standard Classification of Languages (ASCL), 2016

Data Field	Protocols Section	Field Values
Disability, impairment or condition indicator	6.1.8	Intellectual/learning Psychiatric Sensory/speech Physical/diverse None (no disability) Not stated/inadequately described
Consent to have personal information stored in the web-based portal	5.2.3	Tick box
Consent to participate in follow up research, surveys and evaluation	5.2.5	Tick box

*These fields generate an AIHW Statistical Linkage Key (SLK) 581 algorithm.

Table 3. Priority requirements: case level data

Data Field	Protocols Section	Field Values
Case ID	6.2.1	Free text limit of 50 characters. If left blank a system generated number is assigned.
Outlet	4.5	In the web-based portal: to be selected from a list of options in the drop-down.
Program Activity	6.2.1	In the web-based portal: to be selected from a list of options in the drop-down. The drop-down will only display program activities that are assigned to the outlet selected.
Unidentified client count	3.6	Free text number only with limit of 999
Attach clients	3.2	In the web-based portal: to be selected from a list of options in the drop-down. The drop-down provides a mechanism to associate one or more client records to the case.

Table 4. Priority requirements: session level data

Data Field	Protocols Section	Field Values
Session ID	6.2.2	Free text limit of 50 characters. If left blank a system generated number is assigned.
Session date	6.2.2	Date format of dd/mm/yyyy
Unidentified clients attending this session (optional)	6.2.2	Number field. The default value is 0, maximum 999 (however cannot exceed the value specified at the Case level).
Client attendance	6.2.2	Record for each case clients present at the session.
Service type	6.2.2	The number and variety of service types will depend on the program activity selected. The full list of values relevant to the program is in the program specific guidance document on the Data Exchange website.

Table 5. Commonwealth Home Support Programme: client level data

Data Field	Protocols Section	Field Values
Accommodation setting	6.3.1	Boarding house Crisis, emergency or transition Independent living unit Indigenous community/settlement Institutional setting (i.e. residential aged care, hospital) Private residence—client or family owned/purchasing Private residence—private rental Private residence—public rental Public shelter Supported accommodation Other Not stated
Living arrangements	6.3.1	Single (person living alone) Sole parent with dependant(s) Couple Couple with dependant(s) Group (related adults) Group (unrelated adults) Homeless/no household Not stated or inadequately described

Data Field	Protocols Section	Field Values
DVA card status	6.3.1	DVA Gold Card DVA White Card DVA Orange Card or other No DVA entitlement
Existence of Carer	6.3.1	Yes No
Client exit reason	6.3.1	Client no longer requires assistance Service unable to provide assistance Client now requires higher level of care Client has moved out of area Client terminated the service Client died Client no longer eligible Client needs have been met None of the above

Table 6. Commonwealth Home Support Programme: session level data

Data Field	Protocols Section	Field Values
Amount of assistance provided	6.3.1	The information required for this field will depend on the service type selected. Go to the program specific guidance documents on the website to determine which fields apply to each service type: ▪ Hours/minutes ▪ Quantity ▪ Cost ▪ Type
Fees charged	6.3.1	Number field (whole dollars only) appears where applicable

11 Version history

Version 1

The department released version 1 of the CHSP Protocols in July 2025 to advise funded providers of CHSP activities of requirements specific to their program including:

- The requirement to collect My Aged Care IDs from their clients
- Notification requirements for the Mandatory collection of My Aged Care IDs
- Clarify the requirements around conditional on consent storage of personal information (other than My Aged Care ID) in DEX.