Provider Factsheet
Management of Client Records

The Department of Health (the department) is responsible for managing and administering the Australian Government Hearing Services Program (the program).

As specified in the Service Provider Contract (the contract), program client records are owned by the Commonwealth. Contracted Service Providers (providers) must manage, store, transfer and dispose of program client records in accordance with the contract, program legislation, the *Archives Act 1983*, the *Privacy Act 1988* and the *Freedom of Information Act 1982*.

Client personal and health information is deemed sensitive information under the Australian Privacy Principles (APP) and extra precautions are required in the management of this information.

Records Management Policies and Procedures

Ownership and custody

The contract specifies at clause 11.2 that program client records, and any copies of client records, are Commonwealth Records. Clause 11.3 of the contract requires providers to comply with all requests of the Commonwealth in relation to program client records.

- Client records to be transferred to the department when a provider ceases to be contracted by the program or to the new provider when a client relocates. Copies of these client records must not be kept except where required by the contract (for example original claim forms and copies of client receipts under clause 12.3(b) and (c)).
- Transfer of client records does not transfer the ownership of the records.

Access to client records

- Access to client records must be restricted to only those who require it.
- Clients can request access to the personal information held on their client record. Access can be given by providing a copy of the record or by allowing the client to view the record.
- Access to information does not transfer ownership of a client record.

Creation of records

Complete client records consist of all the information relating to a client.

- Complete client records must be accessible and remain complete for seven years from the date of the most recent interaction with the client (the minimum retention period).
- Electronic data (such as in NOAH, Simply Hearing or Fitting Wizard) relating to clients does not need to be combined into a single client record unless the complete client record is requested by the Commonwealth or a new provider when the client relocates.
- Electronic records must also be in a format which is accessible to others (e.g. PDF files).

Digitisation of paper records

The department encourages all providers to move to electronic records. The National Archives of Australia (NAA) guide Digitising accumulated physical records provides useful information and tips on digitisation of paper documents.

- When digitising client records, the entire record must be digitised.
- Digitised records must restrict alteration or record all alterations.
- Digitised records must be in a format which is accessible to others.
- Digitised paper client records must be carefully checked to ensure the record remains complete and accurate. Certification that this check was done must be included with the record. Refer to the Management of Client Records Frequently Asked Questions

Storage

Providers are obligated by the APP (under the Privacy Act) to take steps to protect information from misuse, interference, loss, unauthorised access or disclosure. This includes the use of physical and/or software based security systems.

Whether kept in paper or electronic format, the storage of client records must meet the following requirements:

- confidentiality - access must be restricted to only those who require it
- integrity - must be accurate and complete for at least the minimum retention period
- availability - must be accessible for at least the minimum retention period.

Paper Record Storage

- Paper documents must be kept in a locked cabinet that cannot be accessed by anyone who does not require access and protected by a physical security system.
- If records are removed (for example to take to a visiting site or home visit), they should be locked in a secure, lockable container and kept out of sight.
- The paper used must not be able to be easily damaged or degraded. The use of loose notes (for example sticky notes), should be discouraged. If used they must be secured in a way that will prevent them being lost.
- If client records are required by the department, or another provider for a relocating client, data in systems such as NOAH, Simply Hearing or Fitting Wizard must be printed and provided with the paper file. Providers must have a process in place to ensure the complete record is provided.

Electronic Record Storage

- Electronic client records must be stored in a password-protected system that cannot be accessed by anyone who does not require access, and be protected with security software.
- An Electronic Digital Records Management System (EDRMS) with metadata should be used, rather than a standard computer folder system.
- Electronic documents must be saved in a format which is accessible to others (e.g. PDF).
- If client records are required by the department, or another provider for a relocating client, data in systems such as NOAH, Simply Hearing or Fitting Wizard must be included with the record, in an accessible format. Providers must have a process in place to ensure the complete record is provided.
- Providers must have an electronic record disaster recovery/business continuity plan.

Cloud Storage

Cloud storage allows for shared access to documents via the internet or a company network, but must still ensure the protection of client records. Under clause 17.5 of the contract, program client records must not be taken outside Australia without prior written approval from the Commonwealth. This includes storing client records on overseas servers.

The Australian Signals Directorate (the ASD) no longer certifies cloud service providers and all previous certifications are now void. Providers can continue to use their previously certified cloud services. Any new providers entering the program or existing providers wishing to change their cloud provider or start using cloud services must contact the Program at hearing@health.gov.au before storing client records on a new service.

- Providers must not use unsecured cloud services, such as Google Drive, Google Docs, Dropbox etc, as these may be hosted overseas and do not have Privacy Act protections.
- If providers wish to change cloud providers or start using a cloud service, the security of the service must be assessed. Only an independent Information Security Registered Assessors Program (IRAP) assessor can perform this assessment. Providers should request a copy of a current IRAP assessment of the cloud service before contacting the program.

- Any agreement with a supplier of cloud storage services must include an agreement that the client records will be hosted on an Australian server, will not be disclosed outside Australia and that the records will be encrypted to at least the equivalent of Unclassified with a Dissemination Limiting Marker of Sensitive: Personal or Official with an Access-Information Management Marker of Personal-Privacy.

Non-Program Information

It is a private business decision how pre-program information is held (i.e. records created prior to the client becoming a program client). However, records of private services provided to clients while they are a program client must be kept with the client record. Refer to the Private Services and Devices factsheet for further details.

Backup

To ensure the integrity and availability of client records in electronic storage systems, providers must have disaster recovery and business continuity plans that include the backup of client records.

- Internal (on-site) backup must take into consideration the risk of a disaster occurring at the site and destroying both the original and backup copies of the client records.
- External (off-site) backup must take into consideration the location of the backup server (which must be in Australia) and the backup service disaster recovery and business continuity plans. If a cloud backup is used, it must meet the cloud requirements above.
- Either system must have protections at least equivalent to the storage system, and must restrict access to only those who require it.

File Transfers

- Providers must send complete client records to the department or a new provider when directed by the department. Providers must have a process in place to ensure the complete record is provided.
- Client records can only be transferred between providers where the client has given their authorisation. See the Client relocations provider factsheet.
- Transfer of paper client records must be by registered mail or by courier and must contain a printout of data from systems such as NOAH, Simply Hearing or Fitting Wizard. Data from these systems may also be included on a USB.
- Electronic client records can be sent on a USB drive secured with a password, by registered mail or courier, or by secured and/or encrypted email. The client record must include copies of any results and reports from systems such as NOAH, Simply Hearing or Fitting Wizard in a format that is accessible (e.g. PDF).
- Electronic client records must not be transferred by unsecured email. Email systems are not secure enough for the transfer of personal health information. If a provider wishes to use a secure and/or encrypted email system for the transfer of electronic client records, the location of any storage, the security and compliance with the Privacy Act, the Archives Act and program requirements must be taken into consideration.
- Electronic records must not be printed and sent in paper format. When an electronic client record is printed and then scanned to create a new electronic copy, the quality of the record can become degraded. This does not meet departmental requirements for integrity, and may result in the record or parts of the record being inaccessible for the minimum retention period. The transferred record also must not be split between paper and electronic formats.

Provider Closures

If a provider ceases providing services under the contract all client records that are not to be transferred to a new provider must be returned to the department. These client records must be transferred in the same format as they are held, must not be split between paper and electronic records and any results and reports from systems such as NOAH, Simply Hearing or Fitting Wizard must be included in a format that is accessible (i.e. printed for paper records and PDF for electronic records).

- Providers must not keep a copy of a client record, or part of any client record, except where required under the contract (for example original claim forms and copies of client receipts).

Destruction

Please note from 21 June 2019 there is a freeze on the destruction of Commonwealth records. Providers must not destroy any program client records until the Department of Health advises that the freeze has ended. This includes records of program clients who are deceased or who have not accessed the program for seven or more years.

Where a paper client record has been digitised, and the electronic client record is to become the original record, the source record (paper client record) can be destroyed. Please contact the program via hearing@health.gov.au for requirements.

The disposal freeze on all program client records falls under the terms of reference for the Royal Commission into Violence, Abuse, Neglect and Exploitation of People with Disability.

Providers must hold all records until they are informed they can be destroyed, or they are required for the Royal Commission.

As per section 24(1) of the *Archives Act 1983* (Cth) penalties apply for records disposed of in breach of this freeze order.

More information, including the Notice of Disposal Freeze, is available on the Disposal freezes and retention notices page of the National Archives Authority website.

Data Breaches

Under the Notifiable Data Breaches (NDB) scheme (Part IIIC of the Privacy Act), a notifiable data breach occurs if

- there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and
- the access, loss or disclosure is likely to result in serious harm to any of the individuals to whom the information relates.

If a notifiable data breach occurs, providers must advise the client/s and the Office of the Australian Information Commissioner (OAIC), and follow the requirements under the NDB scheme. Under clauses 20.6 and 24.1 of the contract, the department must also be notified of any notifiable data breaches.

Further information regarding identifying eligible data breaches and determining serious harm is available on the NDB scheme page of the OAIC website.

Compliance Monitoring

Program requirements are monitored in accordance with the program Compliance Monitoring and Support Framework. Where required, the department will notify the OAIC of any identified breaches of the Privacy Act and will follow the instructions of the OAIC in relation to any notified breaches.

Persistent or significant non-compliance with any of the legislative or contractual requirements in relation to program records management may result in referral for compliance actions up to and including actions under Part 6 of the contract (Breach and Termination) and/or referral to the OAIC for actions under Part V of the Privacy Act (Investigations etc.).

Further Information

Answers to frequently asked questions on program records management requirements are available on the program website. Further advice and guidance on general records management is available on the NAA website.