19. Information Management Policy and Procedure

Approval Date: 20 Jan 2020	**Review date:** 20 Jan 2021	**Version:** 1.0

Purpose

Skymac actively works towards implementing and operating effective communication processes and information management systems. We strive to maintain all information systems and practices in accordance with legislative, regulatory compliance and organisational standards.

Scope

It is the policy of Skymac that all participants, staff, volunteers and contractors will have records established upon entry to the service and maintained while active at Skymac.

Policy

- Skymac will maintain effective information management systems that keep appropriate controls of privacy and confidentiality for stakeholders.
- Skymac's policies and procedures are stored as read-only documents in the Policies and Procedures folder on the shared drive.
- Skymac is responsible for maintaining the currency of this information with assistance from other staff as required.
- The involvement of all staff is encouraged to ensure Skymac's policies and procedures reflect best practice and to foster ownership and familiarity with the material.
- A copy of each form used by our organisation is maintained in the shared drive.
- All staff can access the policies and procedures at Skymac's office in a paper-based or electronic format.
- Policies and procedures are reviewed every three (3) years at a minimum, or as required.
- All superseded policies and procedures are deleted from Skymac's Policy and Procedure folder and electronically archived by the Director or a delegate.

Procedure

Skymac information management system

Participant documentation procedure

- Confidentiality of participant records is maintained.
- All Skymac staff and volunteers responsible for providing, directing or coordinating participant support must document their activities.
- Participant's files will provide accurate information regarding their services and support and will contain, but is not limited to:
    - Participant's personal details
    - Referral information
    - Assessments
    - Support plans and goals
    - Participant's reviews
    - Details regarding service responses.
- Original participant documentation is stored in the participant's central file.
- Information relating to a participant's ongoing situation, including changes to their situation, e.g. increased confusion, deteriorating health and increased risks, is to be documented in the participant's notes.
- All Skymac's staff who are required to document the activities relating to support of participants will be appropriately trained in documentation and record-keeping.
- Individuals are not permitted to document on behalf of another person.
- Participant records will be audited regularly to ensure documentation is thorough, appropriate and of high quality.
- Participant records will be stored in a safe and secure location with access available to authorised personnel only.
- Agreements with brokerage agencies will include a requirement for brokerage workers to document their activities regularly.
- Staff must ensure that all relevant information about the progress of, or support provided to a participant, is entered into that person’s file notes in a factual, accurate, complete and timely manner.
- Staff must only use information collected from a participant for the purpose for which it has been collected.
- Participants should be advised that data which has been collected, but which does not identify any participant, may be used by the organisation for a service promotion, planning or evaluation.

- Participants, family and advocates have a right to access any of their personal information that has been collected. Staff will support such persons to access their personal information as requested.

Entering Skymac's service

Upon a participant entering our service all initial information will be collected using Skymac's Participant Intake form. Only personal information necessary to assess and manage the participant’s support needs will be collected.

The Skymac's Assessment Report will be used to document the participant's assessment information.

Skymac's Director will work with the participant, their advocate/s and any other family or service providers/individuals to develop and document a participant support plan; this will be documented using Skymac's Support Plan.

A participant file will be created to act as the central repository of all participant's service information and interactions. A unique identifier will be assigned to each participant for documentation and record-keeping purposes.

The participant's file will only contain material relevant to the management of services or support needs, including, but not limited to:

- Enquiry form
- Copy of signed agreement
- Assessments
- Support plan
- Participant intake form
- Communication notes
- Privacy statement
- Complaint information.

Ongoing documentation procedures

Our ongoing documentation procedures include:

- Maintaining participant information in the electronic Participant Management System, in accordance with system practices
- Documenting participant information and service activities only on Skymac's approved forms or tools
- Ensuring other service agencies and health professionals involved with the care or support of Skymac's participant, provide adequate documentation of their activities and the participant's wellbeing or condition.

The type of detailed information documented includes:

- Outcomes of all ongoing participants assessments and reassessments
- Changes or redevelopment of a participant's support plan, including revised goals or preferences
- Critical incidents or significant changes in the participant's health or wellbeing
- Conversations, in person or telephone, with a participant, family members, their representative or advocate
- Conversations regarding the participant, with any other providers, agencies, health/medical professionals, family members or other individuals with interest in the participant
- Activities associated with the participant's admission and exit, including referrals.

Setting up and maintaining files for participants

Once a personal file for a participant is established, staff must maintain that file to ensure that all information is accurate, up to date and complete:

- Staff must document, in the participant's file, significant issues and events that arise during their work with the participants, as the events and problems occur.
- As information in the personal file becomes non-current (information that no longer has any bearing on the services provided to the participant) staff will establish an archival file and progressively cull non-current information into that file for secure storage.
- The Director must regularly audit the files of participants to ensure that:
    - Files are up to date
    - Forms are being used appropriately
    - Non-current information is being culled and stored in the archival file
    - Progress/file notes are factual, accurate, complete and in chronological order
- When a participant leaves the service, their personal and archival files will be stored in a secure place such as a locked area or password-protected folder on a computer under the control of Skymac.

Participant file formats

- The files of participants will be established and maintained in the following format:
- The file will consist of a standard manila folder, or other similar folder, or held in a secure electronic format with password access.
- The forms must be based on the current formats approved by Skymac.
- Archival files may be in the form of lever-arch folders or archive boxes and multiple in number, as required.

- If files are held in an electronic format, the forms/domains and formats must similarly be approved.
- For ease of access, materials in the archival file should be listed chronologically with each page numbered in order and groups of similar forms.

Security of files and participant information

- All current hard copy files for participants must be kept in a secure area, such as a lockable filing cabinet at the service, ensuring only authorised personnel can gain access to a participant's personal information.
- *Authorised personnel* include Skymac's staff members who are employed to provide support to the participants. If files can't be stored at the service, then alternative arrangements will need to be made by the participant and the Director to ensure confidentiality and security.
- All electronic files must be password protected to ensure confidentiality and security.
- If stored at the service, current files of participants can only be taken from the service by relevant staff from Skymac to provide the participant's information or access to another service, such as a doctor.
- Non-current files should not be removed from the service unless:
    - They are being moved to a more secure archival storage unit
    - Permission has been sought from the Director to do so
- Faxing of information about participants should only be considered in exceptional circumstances. For example, when time constraints prohibit the use of standard security services and only when the receiver of the fax can guarantee the security of the information.
- Staff must not undertake any of the following actions without the express approval of the Director:
    - Photocopying any confidential document, form or record
    - Copying any confidential or financial computer data to any other computer, USB or storage system such as Google Docs
- Conveying any confidential data to any unauthorised staff member or to any other person/s.

Transporting a participant's hard copy files

If, for any reason, the hard copy files of a participant need to be transported from one location to another, e.g. from their usual site to a doctor, the files must be carried in a locked document container, e.g. a briefcase or attaché case. Skymac will provide staff a locked case, as required.

Communication/file notes for participants

- Communication/file notes for participants must include the following components:

    - Date the entry is made
    - Time when the entry is being made
    - Time when the event occurred
    - Nature of the event in a factual, accurate, complete and timely manner
    - Signature of the person making the entry
    - Surname of the person making the entry (printed in brackets)
    - Person's position of employment.
- Staff must ensure that all relevant information about the participant is entered into the person's file notes in a factual, accurate, complete and timely manner.
- The file notes for each participant should be written when a significant event occurs or to record the type of support provided while working with a participant. The definition of a significant event will vary from person to person and should be determined in consultation with the Director and should relate to the support required by the person-centred plan.
- It's required that staff make an entry in the file notes on each workday, even when the person's day has gone according to plan and without the occurrence of unusual or extraordinary events.
- All entries made into file notes should be placed on the next available line. Under no circumstances should blank spaces be left on the file notes sheet.
- All file note entries made by staff, on behalf of another Staff member, e.g. dictating over the phone, must be signed by the person dictating the notes on their next shift. It is the responsibility of that person to check the entry for accuracy and, if required, note any corrections that need to be made on the next line available.
- Whenever required, the participants should be made aware of what has been recorded in their progress/file notes.

Access to participants files

- Participants/guardians are provided access to their records on request. The Director should approve and control the way participants access their files to ensure the security of other non-related information is maintained.
- Access to a participant's file is the direct responsibility of the Director. When access is requested by anyone other than staff employed by Skymac, it will only be granted when the Director is satisfied the policies and procedures of Skymac have been followed and access to the file is in the best interest of the participant. Such access will only be granted when the appropriate person has given consent.
- All participants files are the property of Skymac and although a participant and their guardian can access the file, it cannot be taken by a participant or guardian; or be transferred to any service external to Skymac without permission of the Director.
- Copies of files that are legitimately released for any reason shall be recorded on an appropriate letter, which shall be signed as a receipt by the service recipient or their legal

guardian. The proper procedure for releasing information about a participant to persons or services that are external to Skymac is outlined in our 'Consent Policy and Procedure'.

- Any students on placement at Skymac may only access files with the consent of the participant or their guardian. Students will be required to provide a written undertaking that they will always maintain confidentiality and only use non-identifying information.

This agreement is to specify what information is to be used for and advise that any written compositions containing information are to be provided to the Director for approval before dissemination.

Staff records

Staff files are kept in a filing cabinet in the Director's office and are available only to the Director. The filing cabinet is locked when the office is unattended.

Minutes of meetings

Minutes of meetings are maintained on the shared drive.

Other administrative information

Individual staff are responsible for organising and maintaining the filing of general information in accordance with their job descriptions.

Administrative information including funding information, financial information and general filing are maintained in the filing cabinets in Director's office. The cabinets are locked out of hours or when the office is unattended for a lengthy period.

Electronic information management

Data storage

- All data is stored in the shared drive of the server.
- Director is the only person who can add new data folders to the shared drive of the server.

Backup

- All computer data (including emails) is backed up every night to a remote server.
- Periodic testing of backed-up data is undertaken to check the reliability of the system.

External programs

No programs, external data or utilities are installed onto any workstation without the permission of the Director.

Log-in credentials

Log-in credentials are assigned by the Director or their delegate.

Email

- Staff should send and receive a minimal number of personal emails.
- All emails are filed in the appropriate folders set up by the Director.
- Pornographic, sex-related or spam email received is to be deleted immediately. Under no circumstances are staff allowed to open or respond to spam emails.

Internet access

- Internet access is restricted to work-related purposes.
- Internet access reports are maintained on the server and are regularly reviewed by the Director.
- Under no circumstances are staff allowed to access pornographic or sex-related sites.

4.5.7 IT Support

- Our organisation maintains an ongoing IT support agreement.
- If staff experience problems with a program, computer, or any other piece of IT equipment they can, in the first instance, contact the Director.
- If necessary, the Director will arrange for the IT consultant/s to assist.

4.5.8 Social media

- Our organisation is aware that social media, e.g. social networking sites such as Facebook, Twitter or similar; video and photo-sharing sites; blogs; forums; discussion boards; and websites promote communication and information sharing.
- Staff who work in our organisation are required to ensure the privacy and confidentiality of the organisation's information and the privacy and confidentiality of the participant and their information. Staff must not access inappropriate information or share any information related to their work through social media sites.
- Staff are required to seek clarification from the Director, if in doubt as to the appropriateness of sharing any information related to their work on social media sites.

4.6 Monitoring information management processes and systems

As part of our audit program we regularly audit information management processes and systems. Staff, participants and other stakeholders are encouraged to provide ongoing feedback on issues and areas where improvements are possible.

4.7 Archival and storage

All records, after their active period, must be kept in the archive files for an additional time. Regulatory, statutory, legislative requirements determine the retention period, or alternatively defined by Skymac a s a best practice (refer to ‘Disposal and Archiving of Documents’).

Archived records must be identified and stored in a way that allows for easy access and retrieval when required. Archived records, in hard copy, must be stored in an environment which minimises deterioration and damage, i.e. not exposed to direct sunlight, moisture, extremes of temperature, pests, dust and fire hazards.

4.8 Destruction of records

- The following procedures apply for the destruction of records:
    - Junk mail and instructional post-it notes may be placed in recycling bins or other bins as required.
- All other Skymac records or documents requiring destruction are to be:
    - Shredded and then placed in recycling bins
    - Sent off-site to be securely pulped
- Deleted from the network.

Related documents

- All electronic and hard copy Skymac documentation
- Assessment Form
- Communication notes
- Complaints Register
- Consent Policy and Procedure
- Copy of signed Service Agreement
- Privacy Statement
- Participant Intake Form
- Participant Support Plan

References

- Disability Discrimination Act 1992
- NDIS Practice Standards and Quality Indicators 2020 - Version 3
- Privacy Act (1988)
- Work Health and Safety Act 2011 (QLD)

Disposal and Archiving of Documents

Function/Activity	Description	Retention/Disposal Action	Custody
Aboriginal & Torres Strait Islander	Documents relating to Aboriginal and Torres Strait Islander health Normal operational documents	Lifetime 7 years after the person's last contact with the service	Office
Business Information	Name Address Telephone number Compliance notices Financial records	7 years	Office
Internal Audits	Audit schedule Audit questions Audit reports	2 years	Office
Participant Records	Name Address Telephone number Emergency contact details Application or other documents Complaints about non-delivery of services Incident Records Complaint Records BSP Records	7 years	Office
Contracts/Leases	Properties	7 years	Office
Corrective Action Financial	Corrective Action Requests Audits Budgets Receipts Cheques Petty Cash Documents and other financial records	7 years	Office

Management Review	Minutes of Meetings Monthly Reports	2 years	Held on PCs according to type of meeting