Administration & Information Management Process no: 4.0

Policy:

Efficient and effective administrative procedures are implemented to meet consumer and regulatory requirements. Information is used responsibly to inform the decision making process to improve care and services provided to consumers and effective management.

As a provider of community and home care package services, RusCare is bound to collect personal information according to the Aged Care Act 1997. The organisation is also bound by the Victorian Health Records Act 2001 and the Australian Privacy Principles within the Privacy Amendment (Enhancing Privacy Protection) Act 2012 that set out the requirements for ensuring systems and processes are in place to appropriately manage personal information.

An open and transparent approach to management of personal information is taken and communicated to consumers/their authorised representatives on admission.

RusCare is committed to providing a culture for privacy of personal information and systems for responsible handling of personal information collected. Staff must ensure information is as accurate as possible and must take steps to maintain the security and confidentiality of personal information at all times including but not limited to electronic information, paper based information and oral information such as handover and the use of telephone.

A multidisciplinary team approach to providing care in partnership with consumers and their representatives is provided. Information is only shared with team members on a need to know basis.

Systems are in place to ensure consumer's personal and confidential information related to staff and the management of the organisation is safeguarded against loss, unauthorised access, use, modification or disclosure.

Any individual who suspects a data breach or becomes aware of a data breach must immediately report the incident to their manager.

Response to a breach includes: initial containment and assessment of the breach; if possible, taking remedial action to reduce potential harm to affected individuals; complying with mandatory notification requirements and; reviewing the incident and taking action to prevent future breaches.

A Privacy Officer has been appointed to assist with any issue consumers and their authorised representative/s may have related to privacy of personal information. All matters related to privacy should be directed to the Privacy Officer.

Information and social media technology and social networking must be used according to the IT and Social Media procedure (4.4) to reduce the associated risks to the organisation, consumers and staff.

Steps	Method

A. PERSONAL / HEALTH INFORMATION	• Personal information is information or an opinion about an identified person or who can be reasonably identifiable no matter whether the information or opinion is true or false, or whether it is recorded or not.
	
	• Sensitive information is a subset of personal information and relates to;
	  • Ethnicity or cultural background
	  • Religious beliefs or affiliations
	  • Philosophical beliefs
	  • Sexual orientation or practices
	  • Political opinions
	  • Union / Association membership
	  • Criminal record
	  • Health or medical information.

Administration & Information Management **Process no: 4.0**

Steps	Method

	• Health information is both personal information and sensitive information and has additional privacy protections.
	• Health information is information or an opinion about:
	  • A person's physical, mental or psychological health and or disability with respect to the past, present, future
	  • A person's expressed wishes about future health services
	  • Health services provided or to be provided to a person
	  • Information collected during treatment / care provision, including but not limited to:
	  • The contents of consumer files (paper and electronic) including their date of birth, gender, race, sexuality, religion collected for the purpose of providing care
	  • Prescriptions and pharmacy purchases
	  • Health practitioner appointments and billing details
	  • Consumers' healthcare identifier
	  • Information about a person's suitability for a job, if it contains information about their health.

B. CONFIDENTIALITY	• Staff have the responsibility to maintain confidentiality and to only share privileged personal information about consumers and staff members to other members of the team on a need to know basis.
C. INFORMATION PRIVACY	• Consumers have a right to have their personal information protected through the control of the collection, use and dissemination of personal information as required by the Australian Privacy Principles (APP) and Victorian Health Privacy Principles (HPP). • Information privacy focuses on supporting the control consumers have over personal information about themselves rather than ownership of the information. • Each new Home Care Package consumer is allocated a "Program No" within TCM. • Privacy does not apply to de-identified information for example, statistics where an individual cannot be reasonably identified. • Consumers sign the SCTT consent form and receive a privacy information flyer and the Consumer Information Kit with additional information. • A copy of our Privacy Policy is also available on the RusCare website
D. STAFF PERSONAL INFORMATION	• Whilst the Privacy Act does not cover the handling of personal information by organisations where it is contained in employee records, systems are in place to ensure staff's personal information is safeguarded. • Staff personal information such as; address and phone numbers **must not** to be given to any person outside the organisation.
E. PRIVACY OFFICER	• The Managing Director has been appointed as the Privacy Officer for the organisation and act in accordance with their position description and the organisation's policies and procedures.

Administration & Information Management **Process no: 4.0**

Steps	Method
	• Additionally, RusCare has appointed an external Privacy Officer who may also be accessed in the first instance to resolve privacy issues. • All requests to access or correct information or complaints related to alleged breaches of privacy are to be referred to the Privacy Officer. • Action taken by the Privacy Officer will depend on the individual circumstances of an issue raised and legislative requirements. • An Action Plan (2.0.5) is completed for complex issues to ensure follow up action is planned and completed within defined timeframes. • The Privacy Officer maintains accurate documentation of each issue raised related to privacy. A Privacy Issues Register (4.0.2) is maintained to identify and monitor the progress of privacy related issues within the defined timeframes. • The Privacy Issues Register and related documentation is kept in soft copy format only a secure storage area. • The Privacy Officer refers any matter which is complex or may have legal implications to the Managing Director.

F. AUTHORISED REPRESENTATIVE/ RESPONSIBLE PERSON	• The Health Records Act (Vic) allows for an authorised representative to act for the consumer if she/he is incapable of acting for her/himself.
	• An authorised representative may be:
	  • Enduring Power of Attorney (Financial and Personal) or State Trustee – for finances & property
	  • Medical Enduring Power of Attorney and from 12/03/2018 Medical Treatment Decision Maker and Advanced Care Directives.
	  • Guardian appointed by the Victorian Civil and Administrative Tribunal (VCAT).
	  • Person with written authority or nominated by the consumer.
	
	• The Australian Privacy Act 1988, as amended 2012, allows for a responsible person for an individual to act on her/his behalf if they are unable to do so.
	• A responsible person may be:
	  • A spouse or de facto partner of the care recipient/consumer
	  • A child or sibling of the care recipient/consumer who is over 18 years
	  • A relative of the care recipient/consumer who may be traced to or through a de facto partner, child or sibling e.g. step-child, grandchild, niece.

G. COLLECTION OF PERSONAL INFORMATION	• Sensitive information must not be collected without consumer/authorised representative consent and should only include information required or reasonably necessary for the provision of care and services to the consumer.
	
	• On admission, consumers/representatives are made aware of the following information:
	  • the kinds of personal information required to be collected
	  • how personal information is collected, stored, used and disclosed including any overseas disclosures
	  • how the consumer/authorised representative may access and or seek correction of their personal information
	  • how to make a complaint about any breach of privacy and how complaints will be handled.

Administration & Information Management **Process no: 4.0**

Steps	Method
	• Staff must organise a suitable interpreter for consumers from non-English speaking background, as required.
	• Wherever possible information is collected directly from the individual consumer or representative. • Staff must also maintain privacy when collecting information.

H. QUALITY OF DATA	• Every effort is to be made to ensure information collected, used and or disclosed is accurate, up to date and complete.
	• Consumers/representatives/family members (as appropriate) are encouraged to inform staff if information changes.
	• Entries in consumers' files must be actual and factual about what staff have observed and have done, not their personal opinion of the consumer.
	• The records must comply with legal documentation requirements including;
	  • Consumer's name on each page
	  • Date and time of each entry
	  • No lines left between entries
	  • Signed by the person making the entry and their designation. Nurses must sign according to the name registered to practice.
	  • A Staff Signature Register is maintained to identify initials and signatures.
	  • Whiteout must not be used in any consumer record. Any errors have a line drawn through them and are initialled.

I. USE & DISCLOSURE OF PERSONAL INFORMATION	• Personal Information must only be used or disclosed for the primary purpose for which it was collected; or directly related secondary purpose which would be reasonably expected by the consumer/authorised representative
	• For example:
	  • sharing relevant information between team members to provide the consumer with care and services appropriate to their needs and preferences
	  • sharing information on a need to know basis to service departments
	  • continuous improvement activities including documentation/clinical audits, surveys, reviews and data analysis activities
	  • staff training for employees working within the organisation
	  • handling of complaints;
	  • incident reporting and or legal proceedings for example; assault, professional misconduct.
	  • providing information in an emergency to health professionals for example ambulance officers and locum doctors
	  • submission of funding claims
	  • accreditation assessments.
	• Staff may disclose (communicate) health information related to a consumer to an immediate family member as necessary to provide appropriate care, unless there is an expressed wish that the consumer or authorised representative does not want information discussed with a particular person. This includes general comments to next of kin and close relatives over the telephone.
	• Staff must document such discussions in the progress notes.

Administration & Information Management **Process no: 4.0**

Steps	Method
	• There must be informed consent for use/disclosures for other purposes where reasonable expectation does not apply for example; • Home Care Consumers complete the SCTT Consumer Consent to Share Information form which includes nominating proposed information uses and disclosures. • The consumer/representative must have options explained and have the right to refuse consent for the use of personal information for a secondary purpose. • A consumer/authorised representative may request information to be available to another health service or provide authority for another health service provider to request information. This may involve a copy or summary of the information. • Such requests must be referred to the Privacy Officer and processed as soon as practicable. • Personal information may be disclosed/used for a secondary purpose if it is related to a law enforcement or regulatory purpose for example; subpoena, notifiable disease, compulsory reporting of elder abuse and missing consumer. • Details of such disclosures require documentation including the date, the information was used/disclosed, the enforcement body to whom it was disclosed/used and how it was used/disclosed. • Refer also to Incident Reporting (21.1). • In the case of a subpoena, the whole record is copied prior to sending by Registered Mail to the address requested. • Solicitors requesting copies of records are referred to Managing Director. • Legal advice is sought by the organisation if it unsure about how to proceed with a court order.

J. ACCESS	• Consumers or their authorised representative have the right to access personal/ health information kept by the organisation. The authorised representative must consider whether, if able, the consumer would wish to access the information.
	• All reasonable steps must be taken to provide access.
	• Wherever possible access is provided according to the form the individual requested for example;
	  • Inspection of documents
	  • A copy, ensuring the deletion/omission/protection of personal information related to others
	  • A verbal explanation
	  • A written summary of the information.
	
	• Staff must direct any request to access records to the Privacy Officer who will provide a Request to Access/Correct Information form (4.0.4).
	
	• Upon receipt of a request for access the Privacy Officer will:
	  • Verify that the person requesting access is authorised to do so
	  • Read the relevant documents to which the request relates to identify:
	  ○ Any areas that may require inspection or copying to be denied
	  ○ Information that could cause serious threat to life or effect the health of the person.

Steps	Method
	○ Whether other individuals are identified and require information protected or de-identified. • Prepare a summary or organise the preparation of a summary of the documents, if required. • Organise a meeting with a relevant health professional such as, medical practitioner to provide an explanation, if requested. • Photocopy or organise the photocopying of requested documentation. • Set up a mutually agreed time to inspect or view documents. • Arrange for a private and convenient area to inspect or have the information explained. • An Acknowledgement and Response is provided for all requests using Part B of the Request to Access/Correct Information form (4.0.4) including whether access can be provided or correction can be made and whether a fee applies. Refer below for Refusal of Access. • The applicant will be advised that he request will be responded to within 14 days. Where a response cannot be provided within that timeframe, the applicant will be notified of the reasons in writing.
K. FEES	• Generally a fee is not charged for access unless there is a large amount of photocopying/printing or time required. In these cases: • a fee of 20c per A4 page may be charged for photocopying of records. • a minimum charge of $5/15mins may be charged where staff are required to spend substantial time locating and preparing documents. • Health service providers, such as Medical Practitioners, may charge a fee for providing an explanation. The fee cannot be more than for a usual consultation for the same time. • Where a charge is made by an Intermediary these costs may be shared or waived. • If is believed that the costs of access would pose undue hardship on the person accessing the fee can be waived.
L. REFUSAL OF ACCESS	• Refusal of access is only to occur if access; • Would pose a serious threat to the consumer's life or health. If the threat was removed by providing the information in another form, this should be offered to the person. • Would impact unreasonably on another person. • Relates to information about legal proceedings between the person and the organisation. • The information was given in confidence. • Is unlawful. • Relates to information which would prejudice a security or legal function / investigation for example, a negligence claim. • Has been given and a person is being unreasonable by asking repeatedly to access the same information, in the same way. • Is considered trivial or been made jokingly. • Would leave the organisation vulnerable related to commercially sensitive decision-making information. • However, the consumer is still able to access the facts and opinions and an explanation about how the decision was made related to them.

Steps	Method
	• Where a request for access has been refused the Privacy Officer must provide a reason as required by APP 12 or HPP 6. The Notification of Refusal template letter is used by the Privacy Officer. • An exception to providing a reason would be if the disclosure would prejudice a legal investigation.
M. INTERMEDIARY	• Where refusal has occurred and all other avenues have been explored consider the offer of an intermediary person who is mutually acceptable to the person and the organisation to assist with limited access when direct or limited access is not appropriate. • The Privacy Officer will need to establish whether an acceptable outcome would be achieved for the person with the use of an intermediary without revealing the information covered by the exception. • The Privacy Officer will need to establish the availability of a suitable intermediary. • The Intermediary's role is to facilitate sufficient access, which meets the person's and the organisation's needs. • This person should be another qualified health service provider who will act in the best interest of both parties. • Disclosure of the information to which access has been requested is required with the individual's written consent. This disclosure is to enable the Intermediary to explain the contents of the information to the individual, without revealing specific details without the organisation's authority. • The steps in this process must be explained to the individual when an Intermediary is offered. • The applicant may nominate a consenting health service provider to assess the grounds for refusal if the offer of an intermediary has not been made by the organisation or if they do not accept such an offer or is not satisfied with the outcome of the discussion. A written notice of the nomination must be provided within 21 days after receiving the notice of refusal or an offer or following discussion. • The organisation may object to the nomination in writing within 14 days. • The Privacy Officer will refer to the requirements of the legislation and may require legal advice for this situation.

N. CORRECTIONS OF PERSONAL INFORMATION	• A consumer or authorised representative is entitled to request information to be corrected should they believe personal information is incorrect.
	• Requests for correction are required in writing using the Request to Access/ Correct Information form (4.0.3).
	
	• Upon receipt of a request for correction of information the Privacy Officer will:
	  • Verify that the person requesting correction is authorised to do so
	  • Request supporting evidence to verify the validity of the request.
	
	• Corrected information should be attached as an addendum to the file whenever possible rather than deleting from the file. Incorrect information is to be filed to ensure it is not inadvertently used for example; in the consumer's archive file.

Administration & Information Management **Process no: 4.0**

Steps	Method
	• In rare circumstances an incorrect diagnosis for example, related to psychiatric condition can be permanently erased from the file if the individual expresses a strong concern.
	• If practicable, the name of the person who made the correction and the correction date is recorded on the file where the correction was made. [2(p.136)] • A record of corrections made is also recorded on the Request to Access/Correct Information form (4.0.3).
	• The organisation can refuse to correct the personal/health information if it is believed there is lack of supporting evidence. However, a statement provided by the person should be attached to state that correction was requested. • Where a request for correction has been refused the Privacy Officer must provide a reason as required by APP 13 or HPP 6. The Notification of Refusal template letter is used by the Privacy Officer.
O. COMPLAINTS	• Consumers/authorised representatives have the right to make a complaint where they believe there is a breach of the consumer's privacy. Such complaints must be recorded on a Feedback Form (2.01). and followed up promptly by the Privacy Officer according to the Complaint Handling procedure (2.6) and the Security Breach section below.
	• Consumers/authorised representatives also have the right to make a complaint to the Office of the Australian Information Commissioner/Victorian Health Services Commissioner.
	• The commissioners are able to investigate complaints where it is alleged that there has been a breach of the Australian Privacy Principles/Health Privacy Principles or access has been denied. Compliance notices can be served for serious breaches by the commissioners or binding orders by the Victorian Civil & Administrative Tribunal.
P. RESEARCH / STUDY	• Any request to access medical records for the purpose of research must demonstrate in writing how information will be used and how ethical issues and privacy will be protected. • Written consent using the Consent to Use/Disclose Information form (4.0.3) is required if information is not de-identified or a consent form specifically designed for the research project is used. • Generally where de-identified information is used/disclosed for study purposes no privacy issue arises unless there is no direct relationship between the use and the purpose of the initial collection. In this case; o Consent where possible and feasible should be sought, o How the use / disclosure will tangibly benefit the public health or safety should be demonstrated, o How ethical issues will be addressed should be demonstrated, and o How privacy will be protected should be demonstrated.
Q. MEDIA	• The Managing Director handles media issues for the organisation. All media inquiries are to be directed to this person.

Administration & Information Management **Process no: 4.0**

Steps	Method
	• Personal or health information must not be disclosed unless there is informed consent or expressed consent. • Information may be provided only if individuals cannot be identified by the statement made.
R. FUNDRAISING & DIRECT MARKETING	• The organisation does not use personal information to contact consumers/families for the purpose of fundraising such as donations, bequests or direct marketing without written consent.

S. TRANSFER OF INFORMATION OUTSIDE VIC/AUST	• Information can be transferred if;
	  • Similar information or health privacy principles apply,
	  • The person provides informed consent or,
	  • The transfer will benefit the person and consent is impracticable / the person would give consent,
	  • Reasonable steps are taken to ensure privacy of information for example; a legal opinion,
	  • Required by law.

T. SECURITY OF PERSONAL INFORMATION	• Measures are in place to safeguard personal and health information in any form from loss, unauthorised access, use, modification or disclosure.
	• Physical measures that are in place include but are not limited to;
	  • Staff ensuring filing cabinets are locked when unattended
	  • Staff ensuring desks are clear of personal / health information when unattended
	  • Locked storage area/s for consumers histories with restricted access
	  • Locating white boards with consumer details only in areas where privacy can be maintained
	  • Where Home Care consumer files are taken off site, they must be:
	  • Transported in a secured bag eg brief case in the boot of the vehicle
	  • Not left at any time in an unattended vehicle
	  • Signed in and out of the Client Records Movement Register (53.3.1)
	• Computers are password protected with levels of access. Refer also to Information Technology and Social Media (4.4).

U. PERSONAL INFORMATION SECURITY BREACHES	• The following steps should be taken if there is a situation where personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.
	  • Complete an Incident Report (2.0.2a) and inform the Privacy Officer who will take immediate steps to contain the breach and coordinate the response.
	  • The Privacy Officer will conduct a Risk Assessment (21.0.2) to assess what information has been affected and the risk of harm associated with the breach and if possible the cause and extent of the breach.
	  • The Privacy Officer will then consider if affected individuals should be notified to reduce the risk of harm such as; identity crime, physical harm, humiliation, damage to reputation.
	  • The timing of the notification and method will depend on the level of risk e.g. immediate phone call or letter in the mail.
	  • Notification should include; details of the breach, the type of personal information affected, what is being done to minimise the impact and contact details for information and assistance.

Administration & Information Management Process no: 4.0

Steps Method

- The Privacy Officer will also inform senior management and the need for notifying other agencies or regulatory bodies will be determined for example; the Office of the Australian Information Commissioner (Notifiable Data Breach Scheme, refer to the Notifiable Date Breach Flowchart (4.0.6)), the police, professional or regulatory bodies and or other organisations that maybe affected by the breach.
- A comprehensive investigation is conducted following the incident to identify and if possible implement preventative action such as; increased security measures, staff training, review and update of policies and procedures.

Expected Result/s

Administrative services are provided in a timely manner, meeting regulatory reporting requirements and customer satisfaction. Personal information is collected, stored, used and disclosed according to regulatory requirements.

References

Australian Government Department of Health, July 2019, Aged Care Quality Standards 2018 (St. 1 – Consumer dignity and choice, St. 8 – Organisational governance), (04/07/2019), available at: https://agedcare.health.gov.au/quality/aged-care-quality-standards

Australian Government Department of Social Services Home Care Programme Operational Manual September 2015

Health Records Act 2001, Act No. 2/2001 available at: http://www.austlii.edu.au/au/legis/vic/consol_act/hra2001144/

OAIC, February 2018, Data breach preparation and response, A Guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), available at: https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response

Office of the Australian Information Commissioner (OAIC) Data breach notification - A Guide to handling personal information security breaches, August 2014, available at: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

Office of the Australian Information Commissioner (OAIC), Australian Privacy Principles guidelines March 2015, Privacy Act 1988 (as at 2 March 2018) available at:https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/

Office of the Australian Information Commissioner (OAIC), Frequently Asked Questions – Workplace, available at: https://www.oaic.gov.au/individuals/faqs-for-individuals/workplace/

Office of the Public Advocate, 'Take Control', March 2018.

Privacy Amendment (Enhancing Privacy Protection) Act 2012, No.197, 2012 available at: https://www.legislation.gov.au/Series/C2004A03712/Amendments

Privacy Amendment (Notifiable Data Breaches) Act 2017, No.12, 2017 available at: https://www.legislation.gov.au/Details/C2017A00012

Notifiable Data Breach Flowchart — Form no: 4.0.6

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

Is serious harm still likely?

- NO → Review
- YES → Notify

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.