Supported by

phn COUNTRY SA

An Australian Government Initiative

Digital Health Policy Templates

for Residential Aged Care Facilities (RACFs)

How to use these policy templates

The following set of digital health policies are intended as a guide only and should be individualised to meet the needs of your organisation. We do not recommend implementing these policies without first considering whether they meet the needs of your healthcare organisation and customising them to fit your specific circumstances.

We recommend reviewing each of the policy templates to determine its relevance for your facility. Any individual policies that are not relevant—e.g. if you are using Provider Digital Access (PRODA) rather than Health Provider Online Services (HPOS) and do not require a NASH PKI Certificate policy—can be deleted.

If you are intending to register to use My Health Record, it is a legislative requirement to have a My Health Record policy for your facility.

Once you've reviewed the templates to identify those that are relevant, you should then ensure that each template is adapted to the needs of your organisation and all relevant sections of the template are completed any content changes are made as required.

These policy templates have been adopted from the toolkit prepared by Allied Health Professions Australia (AHPA).

Table of Contents

Electronic medical records administration policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

To provide safe and effective resident care, it is necessary to maintain accurate and up-to date resident records. These must also be secure, so they are not accessible to unauthorised use and backed up in case of a system failure or disaster scenario.

2. Policy

Our facility maintains a resident health record system that suits the needs of our facility, and the administration of this system ensures each resident has a dedicated health record that is complete, maintained, and facilitates the provision of safe and high quality healthcare.

All electronic records are protected from unauthorised access by secure logins and are password protected.

3. Procedure

Our resident health records contain an accurate and comprehensive record of all interactions with our residents.

The facility team can describe how we correctly identify our residents using identifiers (e.g. full name, date of birth, gender, address) to ascertain we have selected the correct resident record before creating, entering or actioning anything from that record.

3.1 Creating a new health record

New residents to our facility are requested to complete a *New Resident Information Form* that is used to gather the resident's:

- Contact information
- Emergency contact details & Next of kin
- Healthcare identifiers (i.e. Medicare/Department of Veterans' Affairs number)
- Cultural identity (including Aboriginal and Torres Strait Islander status)
- Health information (such as allergies, current medications, medical history, lifestyle risk factors)

Once obtained, this information is used to create a health record for that resident.

3.2 Retrieving a health record for a current resident

Our facility has computerised resident records and has systems in place to protect the privacy, security, quality, and integrity of the personal health information held electronically. Members of

the facility team have different levels of access to our resident personal health information as appropriate to their roles.

3.3 Filing reports (pathology, x-ray, consultants, etc.)

Paper-based diagnostic test results and other incoming resident correspondence must be dated and passed on to the referring general practitioner, or delegate if that practitioner is not on duty, and actioned accordingly.

This facility *[amend as appropriate]* scans/does not scan all paper-based correspondence received about residents, with copies of this data securely stored. Original copies are *[amend as appropriate]* retained/not retained.

All results received electronically, are reviewed by the requestor, or delegate if that practitioner is not on duty, and actioned accordingly. These results are then incorporated into the resident's electronic health record.

3.4 Errors in health records

Corrections in the electronic record are to be recorded by referring to the date of the original entry and the associated amendment so that the integrity of the original record is maintained for audit purposes.

3.5 Backup of electronic health records

To avoid lengthy down time, disruption or medico-legal concerns, frequent backups are essential and form a critical component of the facility disaster recovery plan. Systems are backed up daily to [*a cloud-based system OR to a hardware device and stored offsite*] for the purposes of restoring data if required.

3.6 Retention of records and archiving

In our facility, electronic resident health records are retained indefinitely. Resident account records are retained for a minimum of __ years.

Our facility has a process in place to allow for the timely identification of information to be culled, stored, or archived and to enable timely retrieval of records where required.

Deceased records are marked DECEASED and filed in the 'deceased' section of the inactive file storage area.

Privacy and confidentiality is maintained during the destruction process to ensure information contained in the records is not divulged or seen by unauthorised persons. Records will be destroyed by shredding or pulping, in a secure environment. Where a contracted document destruction company is used to undertake this task, certificates of destruction are retained.

4. Related resources

Administrative record keeping guidelines for health professionals | Department of Health

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to aged care providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

Data records and clinical coding policy

Current as of: [insert date of last revision]

Version No: [insert version number]

Our facility ensures that important elements of our residents' health information is recorded in their health record consistently, regardless of the provider they see. The clinical terminologies used are based on agreement by our facility and/or the facility team and we are working towards ensuring the Allied health minimum dataset is included in data collected for resident consultations.

1. Background and rationale

Using consistent clinical coding terminologies will support better utilisation of searchable disease registers and avoid confusion that can result from 'free text' descriptions in the health record. Best facility standards include the use of a medical vocabulary that can be mapped against a nationally recognised disease classification or terminology system.

2. Facility procedure

Our facility:

- discourages the use of free-text coding for the recording of important diagnoses and current and past clinical history in residents' health records.
- is working towards consistent recording by encouraging the use of agreed clinical coding terminologies by using, for example, a 'pick list' or 'drop down box' function in the clinical desktop system
- uses clinical coding terminologies, at a minimum, for all active residents of the facility
- is working towards consistent recording of resident encounters using the Allied Health National Best Practice Data Sets as a guide
- provides facility-based education and skills-based training to all healthcare providers and staff to ensure compliance with the policy and competency in the use of the technology.

3. Software requirements

The clinical desktop system used in our facility is:

[List clinical software]

The medical vocabulary used in the clinical desktop system is:

[List medical vocabulary]

4. Staff responsibility

It is the responsibility of all healthcare providers in our facility, where clinically relevant, to use the 'pick list' or 'drop-down box' capability and reduce the unnecessary and/or inappropriate use of 'free text'.

It is the responsibility of all administrative staff to support the use of clinical coding terminologies by undertaking any administration tasks involved in the maintenance or use of the clinical desktop system. When any problems arise with the clinical desktop system software within our facility, the appropriate software vendor and/or the company providing IT support for the facility will be contacted to assist in resolving the problem in a timely manner.

5. Related resources

| Australian Institute of Health and Welfare

My Health Record conformant clinical software products | Australian Digital Health Agency

Secure messaging policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

Secure electronic messaging significantly lessens the chance of clinical information being accessed and read by anyone other than the nominated addressee. While electronic transmission carries an inherent risk of inadvertent wider broadcast of information, it also offers the opportunity to protect information more efficiently through higher security standards, encryption, audit trails and point to point transmission of data.

2. Purpose

To ensure that our facility utilises standards-compliant secure messaging systems that have the capability to both securely send and transmit clinical messages to and from other healthcare providers.

3. Scope of policy

All messages sent and received that contain clinical information. All health practitioners working within the facility or their nominated representative.

4. Description

Secure Messaging Delivery System – [Insert name of secure messaging software]

All healthcare practitioners within the facility actively use secure messaging (within the clinical software where available) to send, receive and act upon resident clinical documentation/information. Examples of clinical information are referrals to other practitioners, allied health and specialists.

5. Facility procedure

Our facility:

- sends and receives correspondence and reports to and from our clinical desktop system to other healthcare providers using conformant secure messaging software OR if clinical software is not in use in the facility, a stand-alone secure messaging system is used for this purpose.
- supports all healthcare providers in our facility to actively use secure messaging software to send and receive resident documentation, where feasible
- adheres to the use of compliant software to ensure that message contents are encrypted for the entire transmission process using appropriate digital certificates
- has verified that the installed software for secure messaging delivery has been configured in accordance with commissioning requirements

- does not support or condone the use of insecure electronic methods of transmission for communications containing identifiable clinical information (e.g. standard email)
- encourages a sustained increase in the use of standards-compliant secure messaging systems
- where possible uses a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) organisation certificate to facilitate sending and receipt of documents.
- provides facility-based education and skills-based training to all healthcare providers and staff to ensure compliance with the policy and competency in the use of the technology.

6. Related resources

Secure messaging | Australian Digital Health Agency

My Health Record conformant clinical software products | Australian Digital Health Agency

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

My Health Record system policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

To govern the use of the My Health Record system, the My Health Record system Rule states that in order to participate in the My Health Record system, your organisation needs a written policy in place to address access and security issues relating to the use of the system.

2. Purpose

To ensure our facility conforms with the requirements of the *My Health Record Act* by addressing each of the requirements specified therein.

3. Scope of Policy

The policy extends to all AHPRA registered healthcare practitioners working within the facility and administrative staff who have responsibility for maintaining user access to the My Health Record System on behalf of the facility.

4. Description

All healthcare practitioners within the facility actively use My Health Record system to access and upload resident health information as required in the provision of healthcare. Examples of health information that can be accessed and uploaded are allergies, current medications, investigation reports, diagnosis and resident health summaries.

5. Facility procedure

5.1 Managing user accounts:

- An up to date register is maintained, including the names and positions of staff who are authorised to access the My Health Record system
- Healthcare provider software controls ensure access to the My Health Record system is limited to those staff whose duties require them to access the system. Any person involved in an individual's healthcare who is authorised by the healthcare organisation can access a My Health Record.
- Each staff member is provided with a unique user account with individual login details and these details should not be shared with others.
- Staff passwords are regularly reviewed, changed and sufficiently complex i.e. a combination of more than 13 letters, numbers and symbols
- Users are required to deactivate screensavers by entering their username and password or other suitable method of user authentication.

- A user account is immediately suspended or deactivated when a user leaves the organisation, has the security of their account compromised or whose duties no longer require them to access the My Health Record system
- A user account is inactivated/deleted after the departure of the staff member as part of the organisation's off-boarding process
- Where access to the My Health Record National Provider Portal access is required, the organisation maintains a list of up-to-date authorised providers and communicates this with the Australian Digital Health Agency (the System Operator).

5.2 Identification of staff:

- Clinical software is used to assign and record unique internal staff member identification codes, including a Healthcare Provider Identifier-Individual (HPI-I), when applicable.
- The unique identification code, or the provider's HPI-I, is recorded by the clinical software for each instance of My Health Record system access.
- HPOS / PRODA is used to maintain a list of HPI-I numbers for each current staff member requiring access to My Health Record.

5.3 Staff training:

- All staff requiring My Health Record system access undergo training before accessing the system.
- Training is provided and outlines how to use the My Health Record system accurately and responsibly, the legal obligations for organisation and individuals using the system, and the consequences of breaching these obligations.
- Training is provided to staff on a regular and ongoing basis to ensure changes are communicated and understood by all facility team members.
- A register of staff who have attended training is maintained.
- Staff that are not eligible to access the My Health Record understand their obligations in relation to privacy and security of resident information.

5.4 Destroying My Health Record document codes:

- Staff provided with My Health Record security codes (by their residents) to access restricted records and documents within the My Health Record system must not record these within the clinical desktop software system or in any other electronic format.
- If codes are recorded on paper, these documents must be destroyed immediately following the consultation / when no longer required by placing them in locked containers that are removed and shredded.

5.5 Handling of privacy breaches and complaints:

- The organisation has a reporting procedure to allow staff to inform management regarding any suspected security or privacy issues or breaches of the My Health Record system.
- An incident register/log is kept of any suspected breaches, including details of the date and time of the breach, the user account that was involved and which resident's information was accessed, if known.

- A process is in place for the Responsible Officer (RO) or Organisation Maintenance Officer (OMO) to report a breach to the System Operator (the Australian Digital Health Agency).
- If a resident raises an issue in relation to unauthorised access to their My Health Record, the organisation has a complaints management process to take steps to investigate the issue.

5.6 Risk assessments:

- The organisation undertakes periodic privacy and security risk assessments of staff use of the My Health Record system and the organisation's ICT systems generally, and implements improvements as required.
- All risk assessments are documented appropriately.

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

NASH PKI Certificate use policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

A NASH PKI Certificate may be used for a range of reasons including accessing the My Health Record system, securely sharing health information via secure messaging and accessing the NASH directory on the Certificates Australia website. The NASH PKI Certificate for Healthcare Organisations Terms and Conditions require the healthcare organisation to have a set of policies and procedures in place governing use of the NASH PKI Certificate.

2. Purpose

This document describes the policies and procedures that are involved in the usage of the NASH PKI Certificate within *[Healthcare Organisation Name]*.

3. Policy

The policies and procedures stated in this document should be known and understood by everyone within *[Healthcare Organisation Name]* using the NASH PKI Certificate for the organisation.

The NASH PKI certificate for the organisation will be securely stored by the Responsible Officer (RO) or Organisation Maintenance Officer (OMO). This is an electronic file that is password protected and installed in the facility clinical desktop software system.

[Healthcare Organisation Name] will not give its NASH PKI certificate to any other entity or organisation or allow any unauthorised person to use the PKI Certificate, except for any outsourced information technology service provider engaged by it to act as its agent in using its Certificate.

NASH PKI certificates for the organisation should only be used for proper purpose as defined in the NASH PKI certificate terms and conditions.

Individuals who have used the NASH PKI certificates for the organisation understand that they can be identified in respect of each use and the role they performed in respect of that use and are responsible and accountable for this use.

Individuals must notify the Facility Manager immediately whenever the NASH PKI certificate for the organisation is lost, destroyed, stolen, or compromised. *[Healthcare Organisation Name]* must promptly notify the Department of Human Services of the possible loss, destruction or theft of its Certificate, or in the event that *[Healthcare Organisation Name]* considers or suspects that its Certificate has been compromised.

4. Staff responsibility

It is the responsibility of all administrative staff to support the use of NASH PKI certificates by undertaking any administration tasks involved in its maintenance and use. This includes ensuring a current NASH certificate is maintained by the healthcare organisation (NASH Certificates expire 2 years from date of issue) and must be renewed via HPOS / PRODA, downloaded and stored within

the clinical software system to ensure ongoing access to My Health Record and Secure Messaging systems is maintained.

5. Related Resources

ASH PKI Certificate for Healthcare Organisations Terms and Conditions of Use | Services Australia

Request a NASH Certificate | Services Australia

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

Electronic resident communication policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

The Australian Privacy Principles govern the exchange of information to residents including messages sent by SMS, email, fax or other means. Resident consent is required in a documented form before communications can be initiated and health services need to take reasonable steps to protect personal information when using electronic methods of communication.

2. Purpose

Our facility is mindful that even if residents have provided electronic contact details, they may not be proficient in communicating via electronic means and resident consent needs to be obtained before engaging in electronic communication. Electronic communication includes email, facsimile (including eFax) and Short Message Service (SMS).

Communication with residents via electronic means is conducted with appropriate regard to privacy and therefore it is important to have a policy in place to set expectations for staff and residents regarding the use electronic communications tools.

3. Procedure

Our facility's primary reason for communicating electronically withi residents is *[amend as required: to issue appointment reminders, to issue preventative health reminders, to advertise/offer goods or services]* and we verify the correct contact details of the resident *[amend as required: at the time of the appointment being made, when the resident consultation takes place].*

While not encouraged, our facility allows residents an opportunity to obtain advice or information related to their care by electronic means, but only where the practitioner determines that a face-to-face consultation is unnecessary and that communication by electronic means is suitable. Our facility will only provide information that is of a general, non-urgent nature and will not initiate electronic communication (other than SMS appointment reminders) with residents. Any electronic communication received from residents is also used as a method to verify the contact details we have recorded on file are correct and up to date.

Communication with residents via electronic means is conducted with appropriate regard to privacy. Before obtaining and documenting the resident's consent, residents are fully informed through information contained *[insert methods used to ensure residents are aware of the risks associated with engaging in electronic communication]* of the risks associated with electronic communication in that the information could be intercepted or read by someone other than the intended recipient. *As an additional precaution, we will request a resident sends an email to our facility to which we will respond to avoid the risk of sending to an incorrect email address.* Our facility also has an automatic email response system set up so that whenever an email is received into the facility, the sender receives an automated message reinforcing information regarding these risks.

When an email message is sent or received in the course of a person's duties, that message is a business communication and therefore constitutes an official record. Residents are informed of any costs to be incurred as a result of the electronic advice or information being provided, and all electronic contact with residents is recorded in their health record *[specify how the message is recorded in the resident health record].*

4. SMS Messaging and the SPAM Act

When sending SMS messages with the purpose of advertising or offering goods or services at the facility, our facility complies with the *Spam Act (Cth) 2003*.The SMS message:

- clearly and accurately identifies our health organisation as the authorised sender.
- includes accurate information about how the recipient can readily contact the facility.
- contains a functional and clearly presented unsubscribe facility / option to allow residents to opt-out of receiving future messages.

5. Staff responsibility

All members of the facility team are made aware of our policy regarding electronic communication with residents during the staff induction process and are reminded of this policy on an ongoing basis. Staff are made aware that electronic communications could be forwarded, intercepted, printed and stored by others. Each member of the facility team holds full accountability for emails sent in their name or held in their mailbox, and they are expected to utilise this communication tool in an acceptable manner. This includes, but is not limited to:

- limiting the exchange of personal emails
- refraining from responding to unsolicited or unwanted emails
- deleting hoaxes or chain emails
- email attachments from unknown senders are not to be opened
- virus checking all email attachments
- maintaining appropriate language within electronic communications
- ensuring any personal opinions are clearly indicated as such, and
- confidential information (e.g. resident information) must be encrypted.

Only staff members with the appropriate permissions in the software and the necessary training are authorised to send SMS messages to residents and the message details/content are controlled using a template which does not contain sensitive information such as test results or diagnosis/condition details. It is our policy not to respond to resident SMS messages.

Our facility reserves the right to check an individual's email accounts as a precaution to fraud, viruses, workplace harassment or breaches of confidence by members of the facility team. Inappropriate use of the email facility will be fully investigated and may be grounds for dismissal.

The facility uses an email disclaimer notice on outgoing emails that are affiliated with the facility stating *[insert details of the disclaimer notice]*.

6. Related resources

Recommendations when using SMS messaging | Avant

Secure use of email | RACGP

Avoid sending spam | Australian Communications and Media Authority

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

Social media policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

Social media and its use by individuals and organisations is continually growing and user-generated content, such as social networking sites, websites, discussion forums and message boards and blogs also continue to proliferate as forms of information exchange.

As such, RACF staff need to maintain professional standards and be aware of the implications of their actions online. Regardless of whether an online activity is publicly available or limited to a specific group, health professionals need to be aware that information circulated on social media may end up in the public domain and remain there. RACF staff should be aware of their ethical and regulatory responsibilities when they are interacting online, just as when they interact in person.

2. Policy

'Social media' is defined as online and mobile tools and social networks that are used to disseminate information, share opinions, experiences, images and video through online interaction.

Regardless of whether social media is used for business related activity or for personal reasons, the following standards apply to members of our facility team. Team members are legally responsible for their postings online. Team members may be subject to liability and disciplinary action including termination of employment or contract if their posts are found to be in breach of this policy.

3. Procedure

Our facility has appointed *[insert name/position title of the person with designated responsibility for managing the facility's social media]* as our social media officer with designated responsibility to manage and monitor the facility's social media accounts. All posts on the facility's social media platforms must be approved by this person.

When using the facility's social media, all members of our facility team will not:

- Post any material that:
    - Is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, or offensive
    - Infringes or breaches another person's rights (including intellectual property rights) or privacy, or misuses the facility's or another person's confidential information (e.g. do not submit confidential information relating to our residents, personal information of staff, or information concerning the facility's business operations that have not been made public)
    - Is materially damaging or could be materially damaging to the facility's reputation or image, or another individual
    - Is in breach of any of the facility's policies or procedures
- Use social media to send unsolicited commercial electronic messages, or solicit other users to buy or sell products or services or donate money

- Impersonate another person or entity (for example, by pretending to be someone else or another facility employee or other participant when you submit a contribution to social media) or by using another's registration identifier without permission
- Tamper with, hinder the operation of, or make unauthorised changes to the social media sites
- Knowingly transmit any virus or other disabling feature to or via the facility's social media account, or use in any email to a third party, or the social media site
- Attempt to do or permit another person to do any of these things:
    - Claim or imply that you are speaking on the facility's behalf, unless you are authorised to do so
    - Disclose any information that is confidential or proprietary to the facility, or to any third party that has disclosed information to the facility
- Be defamatory, harassing, or in violation of any other applicable law
- Include confidential or copyrighted information (e.g. music, videos, text belonging to third parties), and
- Violate any other applicable policy of the facility.

4. Staff responsibility

All members of our facility team must obtain the relevant approval from our social media officer prior to posting any public representation of the facility on social media websites. The facility reserves the right to remove any content at its own discretion.

Any social media must be monitored in accordance with the facility's current polices on the use of internet, email and computers.

Our facility complies with the Australian Health Practitioner Regulation Agency (AHPRA) national law and takes reasonable steps to remove testimonials that advertise our services (which may include comments about the practitioners themselves). Our facility is not responsible for removing (or trying to have removed) unsolicited testimonials published on a website or in social media over which we do not have control.

Any social media posts by members of our facility team on their personal social media platforms should:

- Include the following disclaimer example in a reasonably prominent place if they are identifying themselves as an employee of the facility on any posting: '*The views expressed in this post are mine and do not reflect the views of the facility/business/committees/boards that I am a member of*', and
- Respect copyright, privacy, fair use, financial disclosure and other applicable laws when publishing on social media platforms.

Social media activities internally and externally of the facility must be in line with this policy.

5. Related resources

Social media guidance | AHPRA

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

Facility website policy

Current as of: [insert date of last revision]

Version No: [insert version number]

1. Background and rationale

Residents are increasingly researching health practitioners online, accessing education and information about their illness or condition online, and taking advantage of opportunities to book healthcare appointments through online platforms.

2. Policy

Our facility is committed to making information about our facility and its services readily accessible for all residents and the community. We regularly update our content to ensure currency of the information and *[Add additional services here e.g. we provide an email address for inbound communications provide a web-based enquiry form]* that clearly states when and how you will respond to a resident or potential resident's enquiry.

3. Procedure

In complying with the *Privacy Act 1988*, our facility provides the following advice to users of our website about the collection, use and disclosure of personal information. The aim of this advice is to inform users of our website about:

- What personal information is collected by our facility?
- Who is collecting the personal information?
- How personal information is used by our facility?
- Access to personal information collected by our facility? and
- Security of personal information collected by our facility?

The facility's privacy policy is posted on the website and is available for download. The website is continually monitored to ensure it is kept current and contains at a minimum the information included on our facility information sheet. Any changes to our facility information sheet are also reflected on the website.

As our website contains advertisements from time to time, we ensure any advertising complies with the AHPRA's guidelines for advertising of regulated health services and includes a disclaimer on any advertising which states that the facility does not endorse the advertised services or products. We also use the AHPRA self-assessment tool to check any advertising for compliance with the guidelines before it is published on our facility website.

4. Staff responsibility

Access to update the facility website is limited to staff that have been assigned this responsibility in their position description and are suitably trained to perform this task.

Updates are approved prior to being published by the facility manager.

5. Related resources

Advertising compliance | AHPRA

Advertising compliance self-assessment tool | AHPRA

Disclaimer

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to your particular facility or circumstances. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to allied health providers, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to residents. Accordingly, CSAPHN disclaim all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.