StarHealth First for your Health & Wellbeing	Related Policy	Client Records Management Policy
	Custodian	Quality Manager
	Approver	GM OSD

PRIVACY PROCEDURE

1. Purpose and Scope

This procedure outlines Star Health's commitment to confirm and uphold our clients' rights to privacy in all respects and to comply with legislation under the Privacy Act (1988) and in particular the Australian Privacy Principles (APPs). Star Health as an entity is covered by the Australian Privacy Principles.

Star Health seeks to uphold the highest standard of client privacy by:

- protecting a client's right to privacy, both within the service and outside the service.
- creating an environment in which clients are confident that their rights are protected.
- guiding the fair and responsible handling of client information, to protect the privacy of individuals' health information and to provide individuals with a right of access to their own health information.

This procedure recognises that all client information held by Star Health is sensitive. Where a staff member has any concerns about a privacy issue they should speak to their manager/coordinator. It covers all clients at Star Health receiving services via staff, contractors, volunteers and students and community members involved in health promotion initiatives.

The procedure specifically covers the following Australian Privacy Principles:

APP 1 – Open and transparent management of personal information
APP 2 – Anonymity and pseudonymity
APP 3 – Collection of solicited personal information
APP 4 – Dealing with unsolicited personal information
APP 5 – Notification of the collection of personal information
APP 6 – Use or disclosure of personal information
APP 7 – Direct marketing
APP 8 – Cross-border disclosure of personal information
APP 9 – Adoption, use or disclosure of government related identifiers
APP 10 – Quality of personal information
APP 11 – Security of personal information
APP 12 – Access to personal information
APP 13 – Correction of personal information

2. Definitions

Term	**Definition**
Anonymity	Anonymity requires that an individual may deal with an APP entity without providing any personal information or identifiers. The entity should not be able to identify the individual at the time of the dealing or subsequently.
Family	Includes the following (without limitation): • a de facto partner of the individual; • someone who is the child of the individual, or of whom the individual is the child; • anyone else who would be a member of the individual's family if someone mentioned in the two points above is taken to be a member of the individual's family
Government related identifier	A 'government related identifier' of an individual is defined in s 6(1) as an identifier that has been assigned by: • an agency • a State or Territory authority • an agent of an agency, or a State or Territory authority, acting in its capacity as agent, or • a contracted service provider for a Commonwealth contract, or a State contract, acting in its capacity as contracted service provider for that contract.
Identifier	An 'identifier' of an individual is defined in s 6(1) as a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual.
Personal Information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable: • whether the information or opinion is true or not; and • whether the information or opinion is recorded in a material form or not.'
Person reported as missing	A missing person is someone: • who has been reported as missing to a locating body; • whose whereabouts are unknown to the locating body, and • who is being sought by the locating body because there are serious concerns for their safety and/or welfare or for the purpose of re-uniting them with their family (but does not include an individual who is being sought): • in relation to legal matters, (including but not limited to), debt, maintenance, support proceedings, wills, child custody, divorce or investigations into suspected criminal activity of the individual, or • for the purpose of genealogical research.
Pseudonymity	• Pseudonymity requires that an individual may deal with an APP entity by using a name, term or descriptor that is different to the person's actual name. Examples include an email address that does not contain the person's actual name, a user name that a person uses when participating in an online forum, or an artist who uses a 'pen-name' or 'screen-name'.
Sensitive Information	• Includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of "personal information" (see above). All health information is sensitive information.

3. Procedure

Regular training of staff in operation of this procedure and in the APPs and the privacy and confidentiality sections of the Health Services Act (Vic) 1988, and the Health Records Act (Vic) 2001 will occur: The Australian Privacy Principles are as follows:

APP 1 – Open and Transparent Management of Personal Information

Star Health will take reasonable steps in the circumstances to implement practices, procedures and systems relating to Star Health's activities that:

- will ensure that Star Health complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and
- will enable Star Health to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

Star Health will have Policies/Procedures/Work Instructions, including this Procedure, as necessary to fulfil requirements in APP 1.

These Policies, Procedures and Work Instructions will cover:

- Types of personal information collected and held;
- How Star Health collects and holds personal information;
- The purposes for which the entity collects, holds, uses and discloses personal information;
- How an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- How an individual may complain about a breach of the Australian Privacy Principles, or a registered app code (if any) that binds the entity, and how the entity will deal with such a complaint;
- Information regarding any likely disclosure of personal information to overseas recipients and the locations and details

Star Health will ensure that the privacy policy is available free of charge and located on the Star Health website www.starhealth.org.au

APP 2 – Anonymity and Pseudonymity

- Star Health will provide an opportunity for clients to contact the organization and enquire about services anonymously, without having to provide personal information.
- Star Health will provide an opportunity for clients to access services using a name, term or descriptor that is different to the person's actual name.
- In the interests of quality healthcare and continuity of care, Star Health will communicate to clients the possible impacts on their treatment of being an anonymous client or using a pseudonym.
- Personal information will not be shared in publics spaces where it can be heard by others, including internalwaiting areas.

APP 3 – Collection of Solicited Personal Information

- Only information which is relevant for providing a service or fulfilling the organisation's responsibility, should be collected from a client.
- Client consent is needed for the collection and sharing of any client information.
- Personal client information should be collected only from the client or a responsible other (e.g. a carer, parent, guardian, spouse or partner).
- Information will be collected in a lawful, fair and non-intrusive way, with consideration given to the individual's circumstances and any cultural considerations.

- At the time of collection (registered clients), or as soon as practicable afterwards, the individual is to be made aware of:
    - The fact that information is being collected.
    - The identity of Star Health and how it may be contacted.
    - The client's right of access to his/her personal record and his/her right to correct it.
    - The purpose of the collection.
    - To whom it may be disclosed, including legal obligations to disclose to relevant authorities or as duty of care.
    - The main consequences if the information is not provided.
    - Whether the supply of the information is legally required.
- The above is the responsibility of service providers, however at Star Health the SAAS team undertake this task by handing out the "Welcome to Star Health" brochure.
- The above does not apply to casual clients, though all other privacy principles and practices apply to their relationship with Star Health
- Clients should be registered by their correct given names, not shortened names or nicknames.
- Clients have the right to be registered as an anonymous client or under a different name or pseudonym and when they elect to do this the consequences of this decision need to be explained by the clinician, especially possible effects on discontinuity of care and possible need to be asked the same questions multiple times (eg allergic reactions). See APP 2.)
- Client information will be collected on the relevant Client Information Management System for the service they are receiving.
- Client information that Star Health receives via a third party, whether solicited or unsolicited, will also be treated according to the same privacy principles and practices as information collected by Star Health.
- Information will be collected in a confidential manner.

Star Health may collect sensitive information about a person reported as missing or may use or disclose personal information about a person reported as missing. If Star Health has a request for information a note must be made of that disclosure on the relevant Client Information Management System. Staff must not collect, use or disclose personal information about an individual who has been reported as missing if they reasonably believe that the collection, use or disclosure of the information would pose a serious threat to the life, health or safety of any individual

APP 4 - Dealing with Unsolicited Personal Information

Unsolicited information is information Star Health did not solicit. When Star Health receives unsolicited client information staff will determine if Star Health would have been permitted to collect the information in accordance with APP 3 and

- If able to be lawfully collected under APP 3, apply APP 5 - 13 in relation to the information (ie as if it were collected under APP 3); and
- If not able to be collected under APP 3, Star Health will destroy or de-identify the information if reasonable and lawful to do so, unless it is part of a Commonwealth record (e.g. My Health Record) where destruction or de-identification is not required.

APP 5 – Notication of the collection of personal information

Star Health will inform people before, or at the time it collects personal information of the following items:

Information about Star Health's Privacy Policy (e.g. found in the "Welcome to Star Health" brochure or on the Star Health website):

- Who is doing the collection and identify Star Health as the collector;

- Types of data and reasons for collection and legal bases of collection;
- Times and methods of collection, for example at first point of contact, assessment, etc;
- Any other organisations who routinely or who may already have provided, information about the person and details of this information and lawful bases for so doing;
- Any information collected by Star Health by compulsion of law;
- Main consequences for people if Star Health does not collect information;
- How people may access or have amended the information Star Health collects which will be included in this procedure;
- How people may complain about a breach of any APP;
- Any overseas disclosure of data and likely countries.

APP6 - Use and Disclosure

- Staff should not acknowledge to others that a person is a client of Star Health.
- Results of tests or other professional information will not be given in the presence or hearing of other clients or staff.
- Names, addresses or phone numbers will not be given to people outside the centre, even if they say they are friends or relatives.
- In response to an enquiry from another organisation the Star Health "Handling Requests for Information Procedure" should be followed.
- Information disclosed confidentially by a client to a staff member should remain confidential unless:
    - **Consented** - the client gives consent for it to be shared with other staff.
    - **Legally required** - the information is such that mandatory reporting or a legal requirement requires disclosure to an appropriate, lawful agency or there is a clear duty of care to disclose. Note: in such cases, Star Health will make a written or electronic file note to this effect.
- Clients or their problems should not be discussed with other (non-treating) staff or other people (other clients, friends or relatives).
- As part of case management it is the usual practice for service staff to discuss client information with other service staff employed by Star Health and outside the organisation involved in shared care. Service staff must ensure that clients understand that this occurs or de-identify the client.

Secondary Purpose Disclosure

- Information that is necessary for the primary purpose for which it was collected, or a directly related secondary purpose that the person would reasonably expect, may be disclosed after general client consent is given. Examples of secondary purposes include:
    - A community health nurse sending client details to the council so they can organise home help.
    - An Occupational Therapist sending client details to builders to get quotes on a bathroom modification.

APP 7 – Direct Marketing

Use of Information in Direct Marketing

Star Health will not use or disclose client, carer or staff information for the purpose of direct marketing if the person has requested orally or in writing that their information not be used for that purpose and will only do so if we:

- Obtain consent from the person in writing; and
- Inform the person of the likely nature and intended use of the information; and
- Provide the person with information on how to withdraw their consent to disclose for direct marketing purposes; and

- Retain a hardcopy or electronic copy of the consent.
- In communications with people about direct marketing, Star Health will always include a reminder that the person can withdraw consent to be involved in direct marketing at any stage, orally or otherwise. Star Health will keep a record of any such communications.

Consent to Receive Direct Marketing

- Star Health will always request and obtain written consent before engaging in direct marketing itself, or allowing others to on its behalf.
- In communications with people about direct marketing, Star Health will always include a reminder that the person can withdraw consent to be involved in direct marketing at any stage, orally or otherwise.

Requests from People to Not Receive Direct Marketing

Star Health will acknowledge in writing or email any requests not to receive direct marketing and will:

- Abide by requests as soon as is practicable
- Keep a record of any communications to or from people regarding direct marketing
- Not charge fees to those applying to not receive direct marketing or to effect the request

APP8 – Overseas Disclosure of Personal Information

As other countries' standards of data protection differ to ours, Star Health will take reasonable steps to ensure an overseas recipient of sensitive information when provided by Star Health does not breach APP8. These steps include:

- Obtaining the person's consent as above; and
- Star Health considering entering into an enforceable contractual arrangement with any overseas recipients to abide by the Act and its principles when:
    - The information is sensitive (as defined in the Act) and adverse consequences are likely from any mishandling of the sensitive information.
    - Star Health has not had dealings with the organisation before or there are reasons to distrust the organisation.

Star Health may disclose information to overseas recipients and not abide by APP8 where required by law to do so.

APP9 – Adoption, use or disclosure of government-related Identifiers and Star Health Unique Identifiers

Government-related Identifiers

Star Health will not adopt as its own identifier a government-related identifier unless:

- It is reasonably necessary to verify the identity of the person;
- It is reasonably necessary to fulfil obligations to an agency or a State or Territory authority (eg Department of Veteran Affairs, DVA, or Centrelink Confirmation eServices)
- It is required or authorised by an Australian law, court/tribunal order
- A permitted general situation exists

Unique identifiers assigned by another organisation (e.g. Medicare and DVA numbers) are not to be disclosed unless it is necessary for Star Health to fulfil its obligations to the other organisation, or the individual's consent to the disclosure has been obtained.

Star Health Unique Identifiers

- **Dental** - all registered clients of Star Health are assigned a unique Dental Record (DR) number when they use the dental service and the Titanium database used according to Dental Health Services Victoria (DHSV) guidelines.
- **Community Health -** a UR number will be assigned clients and data recorded as per Star Health's guidelines for the relevant Client Information Management System.
- **GP –** all medical clients of Star Health will be assigned a unique medical record.
- Clients without a UR number may only receive services provided in a group or as part of a health promotion program as a casual client.
- Clients who do not consent to a registration and a record being made up cannot receive individual services.

APP10 – Keeping Personal Information Accurate, Current & Complete (Quality)

Star Health will take reasonable steps to ensure data it retains and uses is accurate, current, complete and relevant. These include:

- Amendments to personal details of clients are to be updated in the relevant Client Information Management Systems by the Service Access and Support Team or the service provider who collects this information.
- When clients re-present for treatment, the reception team re-confirms and updates basic bio-demographic information which is recorded in the relevant Client Information Management System.
- Clinical information is recorded and updated on the relevant Client Information Management System as indicated clinically.
- Clear writing is to be used on all documents relating to client information and record keeping.
- From time-to-time Star Health will schedule training for clinicians in recording client progress notes and clinical records, including operation of and changes to relevant Acts (eg privacy and client records).

APP11 Security of Personal Information

Star Health will take necessary reasonable steps to secure data from interception, misuse, interference, modification or loss. This includes storage, transport and electronic transmission of data.

Physically Securing Client Records

- During office hours when staff are not in attendance in their offices, all client records or information are to be kept out of sight, in a secure location (e.g. behind a locked door or in a drawer). It is the responsibility of the staff member to ensure files in their possession are kept safely and confidentially.
- Client records (other than dental records) are to be returned to the central client records storage area at each site at the end of the day and are locked away overnight.
- Records carried on home visits, are to be kept in a locked briefcase and carried with Star Health staff at all times. They are not to be left in cars or taken home.
- Personal information that does not need to be kept (eg. photocopies or professional diaries) is to be permanently destroyed, usually by shredding.
- All discussions about clients, whether they are between staff within the organisation, or on the phone, must occur in a confidential environment (ie. in offices, not in reception, corridors or the staff room).

Email and Electronic Transmission (includes S2S)

After a client has consented to release information and this is documented in the client record, personal client information may only be transmitted electronically by:

- S2S/Connecting Care e-referral systems
- Secure email of a PDF file; or

- Facsimile.

When emailing/faxing client information, Star Health will take reasonable steps to ensure information is secure from loss, unauthorised access and modification.

Using Secure Email

The Health Records Act states that entities must take "reasonable" steps to keep information safe when transmitting it outside the organization. One or more of the following steps can be taken to keep email safe:

- Email only PDF versions of text and image documents
- Convert PDF documents to uneditable format where available
- Check PDF files have converted correctly and all pages are correct before sending
- Password protect the PDF file
- Call the intended recipient before sending to alert them to the fact the email is coming – either give the file password here or send via separate email

- Check that "addresses" on emails and faxes match intended recipients before sending
- Activate the "read receipt" option in email software before sending
- Add to progress notes that the email/facsimile was received correctly
- Follow-up emails/faxes not confirmed as received

Further Steps to Securing Email

- The ICT Manager will:
    - Minimise external or remote access to unencrypted emails on server (firewalls, police checks of IT staff)
    - Minimise the number of internal staff that have server access to unencrypted emails
    - Oversee contractor access to unencrypted server emails and take steps to minimise unauthorised access or copying
    - Add suitable disclaimers/warnings to email footers of all staff

APP12 Access to Personal Information

Clients and others have rights to access information Star Health holds about them, but these rights are not unrestricted. Unless there are lawful grounds for denying access Star Health will:

- Upon request by a person (with correct consent) to give access to their own information held by Star Health, give access in a form requested by the person; and;
    - Respond to the request to give access within 45 days of receiving the request, as per the Health Records Act. All requests for access to records are to be handled according to the Star Health "Handling Requests for Information" Procedure

Denying Access to Personal Information

- For requests of access to health-related information, the relevant Program Manager will oversee the access and have the final decision if there are reasonable grounds to deny access.

- However access will not be granted where:
    - There are reasonable grounds that this would constitute a serious threat to the life or health of the client or other individual.

    - Giving access would unreasonably affect the privacy of another

- The request is seen as frivolous or vexatious
- Access would interfere with any legal proceedings or commercial dealings between Star Health and the person

- Denying access is required or authorised by law.

Staff Access to Personal Information

- Access to client records and any other documentation relating to clients is limited to Star Health staff who have a legitimate reason to have access.
- Clients are informed that the record system is used within a multi-disciplinary organisation, so other Star Health staff may have access to their file, particularly if other services are provided.
- If hard client records are used in reception they should be concealed at all times.
- Reception staff who access client information such as appointment books and dairies, must ensure this information remains private.
- Reception staff taking personal details over the phone must exercise care in taking details accurately and discreetly.

APP13 – Correction of Personal Information

- Clients have the right to correct their information if they feel it is inaccurate, out of date, incomplete, irrelevant or misleading. When a client requests a correction to a record the original information is retained, not destroyed.

Retention and Disposal

- Client records or their notes are not destroyed (copies excepted).
- Dental records are archived in the client records room when a client is deceased. All other client records are archived to separate storage, still in UR sequence, in the client records room. Archiving is done at the request of service staff, usually when a client is deceased, has moved to a nursing home, or has become ineligible for services following a move to another area.
- Paediatric records are stamped with an alert to prevent early destruction and should be kept for 25 years. (In readiness for the introduction of scanning of records compliant with the new Evidence Act (Vic) 2008, current Star Health procedure is to retain all client records.
- When a client requests health information to be transferred to another organisation or individual, Star Health will retain the original information and a copy will be sent.

Openness

- All clients have the right to request a copy of this procedure.
- Clients are informed of how Star Health collects, holds and discloses their information. This is achieved verbally by service coordination and in writing by the ”Welcome to Star Health” brochure issued to new clients. Service staff also discuss privacy issues with clients when they gain client consent as part of the registration process.

Training Staff in Privacy and Health Records Act

Regular training of staff in operation of this procedure and in the APPs and the Health Records Act (Vic) 2001 will occur:

- Using the e-Learning, online course developed by the Office of the Health Services Commissioner (OHSC)

4. Related Documents

RELATED DOCUMENTS

- Client Records Management Policy
- Client Records Management Work Instruction
- Consent, Privacy, Rights and responsibilities Work Instruction
- Handling Requests for Information Procedure
- "Welcome to Star Health' brochure
- Staff Code of Conduct
- Consent to Use Photo Form
- Application Form – Health Records Request

5. References

- Australian Privacy Principles APPs (Commonwealth)
- Office of the Australian Information Commissioner (OAIC, Cwth)
- Office of the Commonwealth Ombudsman
- Charter of Healthcare Rights
- Privacy Amendment (Enhancing Privacy Protection) Act (Cth) 2012
- Privacy Regulation 2013 (Cth)
- Tax File Number Guidelines 2011 (Cth)
- Privacy Act (C'wealth) 1988
- Health Records Act (Vic) 2001
- Freedom of Information (Miscellaneous Amendments) Act (Vic)1999
- Carers Recognition Act 2012
- Victorian Charter Supporting People in Care Relationships
- Health Service Act (Vic) 1988
- Privacy & Data Protection Act (Vic) 2014 (formerly the Privacy Act Vic 2000)

6. Document History

(Note: Next review due as per Policy Review Schedule)

Date	Change/ Action	Approved by
November 2014	Initial release	GM OSD
July 2019	Review	GM OSD