CLIENT INFORMATION PRIVACY POLICY & PROCEDURE

Policy Number	CRP002	Version	4.0
Category	CONSUMER RIGHTS	Approving Authority	CEO
Approval Date	NOVEMBER 2013	Next Review Due	NOVEMBER 2024
Review Date	NOVEMBER 2021	Page	Page 1 of 24
Accountable Position	DIRECTOR CAPABILITY AND IMPACT	Policy Framework	INFORMATION SECURITY

1 PURPOSE

The purpose of this document is to provide a framework for Your Community Health ('YourCH') to ensure the privacy and confidentiality of client information and access to this information on request.

Statement of Inclusivity

YourCH is committed to providing an inclusive and accessible environment where people and communities of all identities and backgrounds (including but not limited to, ethnicity, faith, socio-economic circumstance, sexual orientation, gender identity, ability, bodies, migration status, age and Aboriginal and Torres Strait Islander descent) are accepted, safe and celebrated. We achieve this through the guidance of our values and principles.

Human Rights Impact Assessment

YourCH is committed to providing culturally safe and inclusive services and workplaces. We protect the human rights of consumers and staff of all gender identities, sexualities, sexes, cultural backgrounds, faiths and abilities, in accordance with the ***Victorian Charter of Human Rights and Responsibilities*** (2006). This policy and procedure seeks to protect cultural rights through its anti- discriminatory and equitable recruitment practices and processes and protects the right to privacy and reputation and the right to a fair hearing through procedural fairness.

2 POLICY STATEMENT

YourCH is committed to protecting the privacy of client information which the organisation collects, holds and administers.

YourCH uses a range of personal information for the purposes of delivering health services to individuals, and for approved secondary purposes such as funding, management, planning, monitoring, improvement or evaluation, or training provided by the health service to employees or persons working with the organisation.

YourCH recognises the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand, and made accessible to them on the other.

We are committed to:

- Responsible handling of health information, and protecting the privacy of an individual's health information
- Upholding the right of individuals to access their health information, except where this may pose a serious threat to the life or health of the individual or another person
- Respecting the dignity and privacy of the individual, at all times

This policy and procedure document is based on the; Health Records Act 2001 (Vic), the Privacy Act 1988 (Cth) and other legislation (see Legislation). Under the Health Records Act 2001 (Vic) information must be handled in accordance with the 'Health Privacy Principles'. Under the Privacy Act 1988 (Cth), information must be handled in accordance with the Australian Privacy Principles.

YourCH is committed to protecting the privacy of client information which the organisation collects, holds and administers.

YourCH uses a range of personal information for the purposes of delivering health services to individuals, and for approved secondary purposes such as funding, management, planning, monitoring, improvement or evaluation, or training provided by the health service to employees or persons working with the organisation.

YourCH recognises the essential right of individuals to have their information administered in ways which they would reasonably expect – protected on one hand, and made accessible to them on the other.

We are committed to:

- Responsible handling of health information, and protecting the privacy of an individual's health information
- Upholding the right of individuals to access their health information, except where this may pose a serious threat to the life or health of the individual or another person
- Respecting the dignity and privacy of the individual, at all times

This policy and procedure document is based on the; Health Records Act 2001 (Vic), the Privacy Act 1988 (Cth) and other legislation (see Legislation). Under the Health Records Act 2001 (Vic) information must be handled in accordance with the 'Health Privacy Principles'. Under the Privacy Act 1988 (Cth), information must be handled in accordance with the Australian Privacy Principles.

To meet these commitments, we will:

- Only collect personal information from individuals where it is necessary for one or more of YourCH functions or activities
- Collect this information by lawful and fair means, minimising intrusion as far as possible.
- Only use the health information of clients for the purpose for which it is intended or where the client has consented to the use or disclosure, or for a secondary purpose related to the primary purpose and which the client would reasonably expect it to be used
- Ensure as far as is practicable that all health information collected and held is maintained as accurate, complete, up to date and relevant to the purpose for which it was collected
- Take reasonable steps to correct information where information is found to be inaccurate, incomplete, or not up to date
- Maintain client health information in secure client information management databases that protects the information from misuse, loss or unauthorised access
- Provide systems for individuals to access their own health records
- Communicate these systems to users of the health service
- Ensure all staff are provided with the Health Privacy Principles of the Health Records Act 2001 at orientation and are supported to comply with this legislation
- Ensure that all external auditors and contractors comply with Privacy Legislation and YourCH Policy
- Provide training to staff in Privacy and Confidentiality as it relates to health records and personal information
- Act promptly to resolve any complaints regarding the handling of health information, and provide information on complaint resolution mechanisms

- Not disclose any personal information to overseas recipients.

YourCH does not collect sensitive information about its clients unless the client consents and the information is needed to provide a service to the client.

YourCH will appropriately manage any personal information received about an individual that was not sought by YourCH and not needed for the provision of services

YourCH understands that a breach of this legislation by an outsourced or contracted service provider will be taken to have been engaged in by YourCH for the purposes of the Health Records Act.

This policy and its related procedure will be made available on the YourCH website and upon request to clients of the health service without charge.

3 SCOPE

This policy applies to all Board Directors, employees, contracted staff, volunteers and students at YourCH in relation to the health and personal information of YourCH clients.

4 PROCEDURE

4.1 COLLECTION OF HEALTH INFORMATION (Health Privacy Principle 1, Australian Privacy Principle 3)

YourCH only collects health information about an individual for the purpose of delivering a healthcare service to that client. Health information is always to be collected in the least intrusive way possible. YourCH will only collect health information in the following circumstances:

- If the client has consented to the collection of the information
- If required by or under law
- If the information is needed to provide a health service to a client and that person is incapable of providing consent and that individual does not have an authorised representative
- Necessary for research or collection of statistics in the public interest (refer to Ethical Research Policy for further information)
- Necessary to prevent or lessen an imminent threat to the life, health or safety of the individual or the public.

All efforts will be made to ensure that when the information is collected it is collected in a way that is not unreasonably intrusive, and is collected about an individual only from the individual, as far as practicable.

All personal and health information is initially collected and recorded on YourCH client information management systems by the Client Access and Referral Service Team, Client Service Officer or an authorised service provider. As far as is practicable, the information is collected within an environment and in a manner in which supports client privacy and confidentiality.

Sensitive information is not collected or shared except under certain circumstances such as with the client's consent, as provided by law, or to prevent harm. For guidance on collection and management of sensitive information about sexuality or gender, refer to the YCH *LGBTIQA+ Disclosure and Documentation Policy*. For guidance on Child Safe processes, refer to *YourCH Child Safe Policy*.

4.1.1 Notification (Australian Privacy Principle 5)

At the time of collection, or as soon as practicable after, the member of staff collecting and recording the personal information is to advise the individual of:

- How to contact YourCH (phone numbers, address)
- The purpose for which the information is collected
- The organisation having a Confidentiality and Privacy Policy and Procedure that describes:
- the individual's right to access health information
- how the individual can seek correction of information
- how the individual may make a complaint about breaches of Australian Privacy Principles
- Usual disclosures (any other third party that YourCH usually discloses personal information)
- That information is not disclosed to overseas recipients without consent or the disclosure of the information is required by an Australian Court Order
- Where collection is required by law
- Any consequences for the individual if all or part of the information is not provided.

4.1.2 Consent For Collection Of Health Information

Consent must be obtained to collect health information. This may be given verbally or in writing, and may be explicit or implied by the willing provision of information.

- ***TrakCare Consent to Collect***

Service Access staff obtain consent for the collection of information during initial contact or initial needs identification processes. In TrakCare, Service Access staff will check the Consent to Data Collection box in the Referral details screen.

- ***Oral Health Consent to Collect***

For clients accessing Oral Health services, consent to collect information is taken as implied due to attending the service and the client's provision of that information.

- ***Medical Consent to Collect***

All medical clients are assumed to have given consent by attending the clinic. Verbal informed consent or written informed consent is obtained for procedures.

4.1.3 Information collected from a third party

When the information is collected from a third party, YourCH staff must tell the individual whose personal information is collected, the above information as soon as practicable. This also applies in circumstances where the individual may not be aware that YourCH has collected the personal information.

4.1.4 Dealing with unsolicited personal information (Australian Privacy Principle

If YourCH receives personal information about an individual that it did not solicit, and is not required for YourCH to provide a service, YourCH will take steps to de-identify or destroy that information in a timely manner.

4.1.5 Incoming correspondence

The service provider will receive all incoming correspondence relating to client care and: stamp the document, sign and date as read. The original is then sent to Client Records for scanning into the relevant client information management system. Client Records then hold the original in a locked file for seven (7) days to ensure that back-up of the electronic system has been performed by the IT Department.
The original correspondence is then shredded or disposed of securely.

Referrals for specialist medical clinics is scanned into the clinicians' holding bay in Medical Director.

4.1.6 SMS and Social Media

Staff sometimes receive health information from clients via SMS on YourCH mobile phones. When such information is received, the information must be transferred to the client health record and deleted from the mobile device. Staff must not respond to health information received through SMS by SMS (this will mean that staff are resending health information across an insecure mode of transmission). If staff are concerned about the wellbeing of a client based on information received by text message, they should discuss the issue with a Team Leader or Manager.

The only information that should be sent to clients via SMS are appointment details. Clients must only ever be provided with YourCH phone numbers and mobile numbers. Personal mobile phone details must never be provided to clients.

At no time should social media sites (e.g. Facebook and Twitter) be used to relay health information or other confidential information. These sites are in the public domain and therefore offer no security.

4.1.7 Information collected under Australian law or court order

If the collection of personal information is required by Australian law or a court order, this must be communicated to the individual. The notification must inform the individual that collection is required or authorised, and should include the name of the relevant law or details of the court or tribunal order that requires collection.
The individual will not be notified if the information is legally required as part of an ongoing investigation and notifying the individual would jeopardise the investigation.

4.2 USE AND DISCLOSURE (Health Privacy Principle 2, Australian Privacy Principle 6)

4.2.1 When information may be disclosed

Identifiable health information is only to be disclosed or transferred where:

- the individual has given their consent for this to happen, either expressly or implied and the recipient is a health service provider providing a health service to the individual
- it is believed that use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health, safety or welfare, or a serious threat to public health, safety or welfare
- use or disclosure is required, authorised or permitted by or under law (e.g. Subpoena, warrant from the Health Services Commissioner, the Forensic Leave Panel, Victorian Civil and Administrative Tribunal (VCAT) or the purposes of an inquiry into a child death to the Child Safety Commissioner, Serious Incident reporting, National Disability Insurance Scheme (NDIS) Commissioner, Aged Care Commission).
- unlawful activity is suspected, or the information is necessary for a law enforcement function
- it is known or suspected that an individual has been involved in an emergency or disaster, and may be injured, missing or dead as a result, and the use or disclosure is necessary to identify the individual
- disclosure is for a secondary purpose, directly related to the primary purpose for which it was collected, and the purpose is one for which the client would reasonably expect the information to be used such as for the purpose of funding, management, planning, monitoring, improvement or evaluation; or training provided by the health service to employees or persons working with the organisation.

4.2.2 Consent For Sharing Health Information

TrakCare Consent to Share
Service Access staff document the client's consent for the information collected to be transferred to the care provider in TrakCare. This consent is documented in the Consent for Referral box in the Referral Details screen.

At all other times when information is transferred to another care provider – either internally or externally – consent to share should be documented ~~-~~in the progress notes. Consent forms do not need to be included in referral information sent to another provider. The Department of Health (2012) notes that it is the duty of care of the service sending the information to ensure that informed consent is obtained.

Oral Health Consent to Share
Consent to share for the purpose of referral is documented in the progress notes.

Medical Consent to Share
It is YourCH's responsibility to ensure all referrals to other services have consent recorded either on hardcopy attached to the file or verbal consent recorded in the client's notes.

4.2.3 Disclosure to immediate family member

YourCH will only disclose health information about an individual to an immediate family member of the individual without their consent if:

- the disclosure is necessary to provide appropriate health services or care to the individual *or*
- the disclosure is made for compassionate reasons, *and*
- the individual is incapable of giving consent to the disclosure and the disclosure is not contrary to any wish expressed by the individual prior to becoming incapable of giving consent
- legal provisions exist granting authority such as a medical power of attorney or guardianship arrangement
- the information is genetic information that the organisation has obtained in the course of providing a health service to the individual and the organisation believes that the use or disclosure is necessary to lessen or prevent a serious threat to life, health or safety of another individual who is a genetic relative.

4.2.4 Disclosure for clients who are minors

The AMA *Guidelines for doctors on disclosing medical records to third parties (revised 2015)* states that: "some minors are capable of consenting to medical treatment. The law recognises that these minors, who have sufficient intelligence and understanding, are capable of consenting to medical treatment. The confidentiality of these minors should be respected; therefore parents may not have automatic access to their medical records without the consent of those minors." (p.2)

It is recommended that except in circumstances of a medical emergency:

- if a minor is not capable of consenting to their own treatment, generally ~~the parent/~~guardian or ~~-~~medical treatment decision maker may access the medical record and provide authority for disclosure to a third party
- where parents are separated or where there are child protection issues, consent of both parents/guardians should be sought where practical
- if a parent/guardian asserts a sole right to authorise disclosure, the care provider should seek a written explanation of that assertion and may wish to seek their own legal advice on its correctness (this may be in the form of a parenting order)
- if a Family Court order has specified parental responsibility to be exercised by one or both parents, this order should be sighted.

4.2.5 Individual may authorise another person to be given access

The organisation must give the person named access to the health information if an individual:

- has a right of access; and
- has signed a written authority for access to be provided to a person named in the authority

4.2.6 Sensitive information

Sensitive information is never disclosed to a third party unless directly related to the provision of a service.

4.2.7 Recording disclosure of health information for the purpose of law enforcement

If health information is disclosed for the purpose of a law enforcement function, a written note of the disclosure must be noted in the client record.

4.2.8 Confidentiality of Persons Under Health Observation

The National Focal Point is an entity established under the National Health Security Act 2007 to monitor health security risks. It is a designated area within the Department of Health and Ageing for International Health Regulations this is responsible for liaising and facilitating actions relating to national or international public health events.

- If a person is placed under public health observation, and that person's personal health information is documented, then YourCH may only disclose that information:
- if required to do so by the Minister or the National Focal Point;
- to a court, tribunal or coroner, for the purposes of proceedings including a coronial inquiry;
- if authorised or required to disclose that information in accordance with a law of a State or the Commonwealth; or
- for any other purpose authorised by the Minister.

4.3 DIRECT MARKETING (Australian Privacy Principle 7)

YourCH does not use personal information about an individual for the purpose of direct marketing. Information about YourCH services is only mailed directly to the members of YourCH as part of their membership.

4.4 HEALTH INFORMATION AND RESEARCH

Health information may be disclosed for the purpose of research or the compilation of statistics in the public interest if:

- it is impractical for the organisation to seek the individual's consent; and
- the purpose cannot be served by using de-identified information; and
- the use or disclosure is in accordance with any guidelines issued by the Health Services Commissioner; and
- the organisation reasonably believes that the recipient of the information will not disclose it; and
- the disclosure will not be published in a form that identifies particular individuals or allows for their identity to be ascertained

For YourCH to rely on the Guidelines from the Health Services Commissioner to lawfully collect information, the research must have been approved by a Human Research Ethics Committee (HREC).

Note that the overriding obligation is to at all times respect the dignity and personal privacy of the individual. Consent may only occur if the individual has the capacity to consent. Consent

must be voluntary, informed, specific, and current. (see YourCH *Shared Decision-making and Informed Consent Policy*).

Refer to the YourCH *Ethical Research Policy* for further information about health information privacy and research.

4.5 DATA QUALITY (Health Privacy Principle 3, Australian Privacy Principle 10)

YourCH will take steps to make sure that the health information we collect, use, hold or disclose is accurate, complete, up to date and relevant to its function or activities. This is done through regular documentation audits and by ~~clinicians and~~ staff working within their scope of practice. All staff sign a code of conduct and are required to abide by the privacy expectations outlined within this code of conduct.

4.6 SECURITY AND RETENTION OF PERSONAL AND HEALTH INFORMATION (Health Privacy Principle 4, Australian Privacy Principle 11)

YourCH ensures the security of personal and health information that it collects to provide a service or other operational function by the following means:

4.6.1 Verbal Information

All discussion about clients whether amongst staff within the service or over the phone should not be conducted in the presence of or overheard by unauthorised persons. All staff must be careful not to talk about their clients in corridors, waiting rooms and other public areas within or outside the Service. All client interviews, medical examinations and treatments should be carried out in privacy and with discretion as far as practical. Information with regards to client's whereabouts at the Service must not be released to anyone unless the client has given permission. If a person requests to know clients whereabouts, reception staff need to phone client's worker discretely and advise them of name of person inquiring.

4.6.2 Computer Information

Computer access by staff for client information is obtained via password. All efforts should be made to reduce casual observation of computer screens, by minimising or locking the screen whenever not directly entering information. Refer to YourCH *Information Management Policy and* YourCH *Acceptable Use of Telephony, Computer, Internet, Intranet and Communication Policy.*

4.6.3 Hard copy health information

Written information includes client health records and all correspondence related to clients such as reports and letters. Client health information must not be left unattended or in unsecured environments. Any working notes that identify clients that are kept in unattended offices must be secured in locked areas. All staff must ensure that keys to filing cabinets have duplicate keys kept in administration.

When conducting home or community visits, records must be kept secure and notes made within 24 hours. Records are to be contained in a secure discrete location during transport to and from visits, e.g. under the seat out of sight or locked in the vehicle boot and an unmonitored vehicle must be locked.

4.6.4 Secure transfer of information

Staff at YourCH must only transfer client health information via personally addressed mail, secure websites, encrypted e-mail software or fax. Internet-based file sharing software is not to be used to share confidential information (e.g. BitTorrent, Dropbox).

4.6.4.1 *Email*

No identifiable health information is transferred external to YourCH by general e-mail. Staff at YourCH may only transfer identifiable health information via general email internally as the internal email is encrypted at both ends. Email may be used in the following circumstances:

- Where a client and/or service requests AND;
- The client has been informed of the risks associated with transfer of information by email i.e. email is not a secure means of transmitting information, and as such may be intercepted or altered by a third party AND;
- The client – with this knowledge - has consented to the transfer of information via email.

The email must contain the following disclaimer:

> *Disclaimer:*
> *This email, including any attachments, is only for the intended addressee. It is subject to copyright, confidential, and may be the subject of legal or other privilege, none of which is waived or lost by reason of this transmission. If the receiver is not the intended addressee, please accept our apologies, notify us by return email, delete all copies of this email, including any attachments, and perform no other act on the email. Unfortunately, we cannot warrant that the email has not been altered or corrupted during transmission. Generally information which passes over the internet is not secure. The confidentiality or security of any personal information using email cannot be guaranteed. Any personal information in this email must be handled in accordance with the Health Records Act 2001 (Vic) and the Privacy Act 1988 (Cth).*

Do not:

- Include confidential information in the subject line or body of the email
- Send information to or from free web-based email accounts such as Gmail, Hotmail, or Yahoo! (even with above protections). These web-based accounts are often owned by international companies in foreign jurisdictions.

4.6.4.2 *Facsimile (Fax)*

Faxes are generally used as a secure means of transferring client health information between YourCH and external service providers. Client information including letters, laboratory results/reports, discharge summaries, examination reports, should be transferred by fax only. While confidentiality of faxed information cannot be assured because of the possibility of reaching the wrong number, or the unknown, it is considered a more secure method of transferring client information than general e-mail.

When it is considered necessary to fax client information, the following procedure should be followed:
Contact the client verbally or in writing to obtain consent. Where the consent is verbal a file note is to be made in the progress notes.
Use a fax cover sheet (found on the intranet) which clearly identifies the sending agency and contains the following:

- Date and time of transmission
- Total number of pages
- Destination : name of agency, fax number
- Person and department nominated as recipient
- Person and department sending fax, and telephone number
- The word "CONFIDENTIAL" prominently placed on the cover sheet
- Ensure the correct fax number has been dialled and connected.
- *When sending a fax to settings where you are not sure the information will be secured on receipt, you must arrange for there to be someone on the receiving number who is*

alerted to the arrival of the fax so they can ensure confidentiality of the information on receiving the fax.

- Scan the fax confirmation sheet into the relevant electronic health record.
- Record details of information released, by whom, and to whom in the client's health record.

4.6.4.3 *Other written correspondence*

Except for the medical team, all electronic copies of correspondence relating to clients are only to be created and stored temporarily in protected YourCH electronic drives where permissions limit access. Correspondence must not be saved to any other drive on the YourCH network. All correspondence must be attached into the relevant client electronic health record in the relevant client management system.

All correspondence created by the Medical Practice is created and stored in Medical Director. No Medical Correspondence is to be created or saved on the YourCH network.

For other services at YourCH, any correspondence created in Word is to be immediately printed, then signed by the service provider. The service provider must take a copy of the correspondence and send to Client Records for scanning into TrakCare.

The service provider mails the signed original to the intended recipient.

Alternatively, staff may use their electronic signature to sign correspondence created in Word. Where the electronic signature is used, staff may attach (upload) the correspondence into TrakCare and print and send a hard copy to the client.

Confidentiality of information sent from other service providers needs to be ensured once it has been received. Concerns about the overall confidentiality of information should be raised with service providers who are sending information in unsecured formats.

4.6.5 Information from a Third Party that is to remain confidential

If personal information about an individual is given to ~~a Youra~~ YourCH service provider by a person other than the individual, with the request that the information not be communicated to the person to whom it relates, the service provider must record the information:
Only if it is relevant to the provision of health services to the individual and
Only if the provider has taken reasonable steps to confirm the accuracy of the information
With a note in the progress notes section of the electronic health record that the information was given in confidence and is to remain confidential.

4.6.6 Personal information that is no longer required

Personal information about an individual that is no longer required to deliver a service and does not need to be retained to comply with Australian legislation or a court or tribunal order must either be destroyed or de-identified.

Refer to the YourCH *Client Health Records Policy* ~~and Procedure,~~ for more information on management of health records.

4.7 OPENNESS (Health Privacy Principle 5, Australian Privacy Principle 1)

YourCH will make this policy available to anyone who requests it, ensure that information about our privacy practices is available publicly on our website and that information about client rights and will be made available as per section 1.

4.8 ACCESS TO PERSONAL AND HEALTH INFORMATION (Health Privacy Principle 6, Australian Privacy Principle 12)

YourCH must provide an individual with access to their personal information if requested by an individual unless:

- it is believed that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety
- giving access would have an unreasonable impact on the privacy of other individuals
- the request for access is frivolous or vexatious
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations
- giving access would be unlawful
- denying access is required or authorised by or under an Australian law or a court/tribunal order
- both of the following apply:
- YourCH has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and
- giving access would be likely to prejudice the taking of appropriate action in relation to the matter
- giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process

4.8.1 Forms of access to the health record

Access to the health record may occur in the following ways:

- inspection of the health information or, if the health information is in an electronic form, a print out of that information, and having the opportunity to take notes of its contents
- the provision of a copy of the health information
- the provision of an accurate summary, instead of a copy, if the organisation and the individual agree that a summary is appropriate; or
- an opportunity to view the record, accompanied by an explanation of the information.

Interpreting services will be made available if required to facilitate the process.

4.8.2 Process of application for access to health record

Clients (or their representatives) who wish to access their record may apply to access their record using the *Health Record Access Form.* The form must be completed and signed by the client or their authorised representative and a 100-point identity documents (detailed on the form) provided. Records are not released without completion of the form and provision of 100-point identity documents.

The completed form is to be forwarded to the Health Information Officer who will check the client information management systems and then forward to the relevant program manager for review and authorisation of release of the information, in consultation (where possible) with the clinician who created the record.

The relevant program manager will then liaise with the Health Information Officer to ensure the secure transfer of the record either via registered post or fax.

Where the health record indicates complexity, including in the following situations:

- The person whose record is requested is deceased
- The request is made by an individual other than the client themselves

- Family court orders or other administrative orders are in place
- The program manager is to escalate the review and release of the record to the Director Capability and Impact.

4.8.3 Fees associated with access to documents

Fees may be charged for granting access under the Health Records Act. YourCH uses the Fee schedule set out in the Health Records Regulations 2012. The maximum charges in August 2021 were:

- A fee of 20c per page for A4 black and white copy of the record
- A fee of no more than $17.80 per half hour for time spent supervising inspection or viewing of the record
- A fee of $67.00 for assessing and collating the information
- Postage costs (if the record is posted).

Refer to the fee schedule set out in the Health Records Regulations to confirm current charges.

Clients are to be notified if they will be charged for access.

Where a fee is to be charged, payment of that fee must be received before the release of the medical record.

4.8.4 Second opinion about "serious threat"

If a request to access health records is refused on the grounds of access presenting a serious threat to the individual making the request, the individual nominate an independent health service provider to provide a second opinion. YourCH may also suggest an independent provider to give a second opinion.

4.8.5 Timeframes for responding

YourCH must respond as soon as practicable and provide access within 45 days, in a form that is requested by the individual. If the request is refused due to one of the exceptions listed above, YourCH must explain in writing to the individual the reasons for refusal provided that it is safe and reasonable to do so, and the mechanisms for making a complaint about a refusal (see section 14.2 Complaints).

4.9 CORRECTION OF PERSONAL OR HEALTH INFORMATION (Health Privacy Principle 6, Australian Privacy Principle 13)

Clients have the right to seek correction of their health information record. If it is found that health information held by YourCH about an individual is out-of-date, inaccurate, incomplete, irrelevant or misleading, YourCH must take steps to correct that information.

If an individual requests that their personal information be corrected, YourCH must respond to the request within 30 days of the request being made. If YourCH refuses to correct the personal information, it must explain in writing to the individual the reasons for refusal and the mechanisms available for making a complaint about the refusal. (See section 4.16).

If the request is refused, the individual may request that a statement regarding their view that the information is inaccurate, incomplete, irrelevant or misleading be linked to the relevant information. This must be done in such a way that the statement is apparent to other users of the information.
See also YourCH Client Records Policy and Procedure for information regarding corrections to client progress notes.

4.9.1 Notification of correction to third parties

YourCH must take reasonable steps to notify any third parties using information that has been previously disclosed and subsequently corrected, of the correction.

4.10 IDENTIFIERS (Health Privacy Principle 7, Australian Privacy Principle 9)

YourCH clients are assigned a unique identifier which enables the service to operate efficiently and increases the safety of service delivery to its clients by ensuring the recording of health information occurs in the correct client health record. The unique identifier is used as one form of identification of the client. Client identification is to be completed and recorded ~~F~~or the purposes of correct identification of a client for:

- Providing services/supports,
- Providing clinical care or therapy,
- matching clients with procedures,
- prescribing, dispensing or administering medication,
- transfer of care
- ~~or~~ referral to internal or external services.

Each time client identification occurs, at least three approved client identifiers are to be used. This provides manual and electronic patient identification systems with the best chance to correctly match a client with their record, without imposing impracticable demands on information gathering.

The preferred primary identifiers are listed in order of preference below:

- Full name (family and given names)
- Date of birth
- Home address in full
- contact phone number
- Gender
- Health Record Number or Individual Healthcare Identifier

Refer to YourCH *Client Identification and Procedure Matching Policy* for more detail on client identification.

4.10.1 Adoption, use or disclosure of government related identifiers

YourCH does not adopt government-related identifiers to use as its own identifier of individuals. Examples of government-related identifiers include driver's licence number, Medicare number, or a DVA File Number. These identifiers are only to be used or disclosed with the individual's consent to confirm eligibility for services.

4.11 ANONYMITY AND PSEUDONYMITY (Health Privacy Principle 8, Australian Privacy Principle 2)

YourCH recognises the right of clients to remain anonymous or use a pseudonym where this is practicable and safe.

4.12 TRANSBORDER DATA FLOWS (Health Privacy Principle 9, Australian Privacy Principle 8)

Health information may only be transferred outside of Victoria if YourCH believes that the recipient of the information is subject to laws substantially similar to the Health Privacy Principles of the Health Records Act 2001.

Personal information must not be disclosed about an individual to an overseas recipient, unless:

- the disclosure is required or authorised by an Australian law or a court/tribunal order
- the individual is informed that YourCH will not be able to ensure the overseas recipient does not breach the Australian Privacy Principles, and having been informed, the individual consents to the disclosure.

4.13 TRANSFER OR CLOSURE OF YOURCH (Health Privacy Principle 10)

If YourCH is to be sold, transferred, or closed down it will give notice of the closure to individuals who have received health services from YourCH in accordance with the Health Records Act (VIC) 2001.

Individuals will be able to have their health records transferred to themselves or another health service provider. If no request is received, YourCH will deal with the health records in accordance with the Health Records Act (Vic) 2001.

4.14 MAKING HEALTH INFORMATION AVAILABLE TO ANOTHER HEALTH SERVICE PROVIDER (Health Privacy Principle 11)

If an individual requests YourCH (or authorises another health service provider to do this on their behalf) to make their health information available to another provider, YourCH must comply with the request as soon as practicable by providing a copy or written summary of that health information to the other health service provider. The individual must complete a *YourCH Health Records Access Form* (found on the intranet and website) prior to releasing that information.

YourCH staff requesting information about a client from another health service provider may make the request by completing the YourCH *Consent to Release Health Records to YourCH Form* (found on the intranet).

4.15 DEALING WITH THE NATIONAL CANCER SCREENING REGISTER

The National Cancer Screening Register Act 2016 provides for a healthcare provider to "collect, make a record of, disclose and otherwise use" personal information or key information for an individual if the person does so:
for the purpose of including information in the National Cancer Screening Register
the information is about screening or diagnosis in relation to the individual
the collection, use and disclosure is for the purpose of providing treatment to the individual for the designated cancer.

This provision is made for the purposes of other laws, including the Australian Privacy Principles.

4.16 REPORTING BREACHES AND COMPLAINTS

4.16.1 Breaches of Confidentiality

A breach of confidentiality can include staff members talking about clients when it does not relate to the provision of care; clients overhearing private consultations; or unauthorised people seeing health records when they have no business seeing them.

Staff members will have to use their judgement and sensitivity in determining how to deal with situations, e.g., when a third party (adult or minor) is present with the client.

Intentional breaking of confidentiality of client information is a serious breach of duty and the YourCH *Code of Conduct Policy*.

4.16.2 Reporting breaches of privacy and confidentiality

Suspected breaches should be discussed with the Team Leader in the first instance and should be reported as an incident in VHIMS.

Under the service agreement with the Department of Health and Department of Families, Fairness and Housing, all privacy and confidentiality breaches must additionally be reported to the Department of Health. This notification must happen immediately (within one business day) when the organisation becomes aware of a breach or possible breach of obligations under the *Privacy and Data Protection Act 2014* or the *Health Records Act 2001.* The report is to be made by the Director Capability and Impact in consultation with the CEO via a web-based form hosted by the Department.

4.16.3 Complaints

A client may make a complaint about the quality of the health record or a decision relating to access to the medical record via the YourCH *Have Your Say Form* or online using the feedback page of the YourCH website. A complaint in writing can also be made at any time to the Victorian Health Complaint Commissioner (HCC), or to the Federal Office of the Australian Information Commissioner (OAIC).

The Victorian Health Complaint Commissioner receives and resolves complaints about health service providers with a view to improving the quality of health services for everybody under the Health Records Act (VIC) 2001. Information about the process for making a complaint about possible breaches of privacy through the HCC is available on the website: https://hcc.vic.gov.au/ or phone 1300 582 113.

The Office of the Australian Information Commissioner has complaint handling responsibilities under the Privacy Act 1988. Information about the process for making a complaint about possible breaches of privacy through the OAIC is available on the Commission's website at: www.oaic.gov.au or phone 1300 363 992.

Complaints may also be made to the Officer of the Commissioner for Privacy and Data Protection.

Complaints to the CPDP must be made in writing. You can make a complaint using:

- the secure online form at https://www.cpdp.vic.gov.au/menu-privacy/privacy-public/privacy-public-make-complaint
- by mail
- by fax
- by email to privacy@cpdp.vic.gov.au

YourCH Directors, management and staff must cooperate fully with any investigation into complaints or possible breaches of privacy by the HCC, the OAIC or the CPDP.

4.17 CONFIDENTIALITY AGREEMENTS FOR WORKERS OTHER THAN STAFF

Each of the following individuals read and sign a Confidentiality and Privacy Agreement that commits them to complying with relevant legislation and YourCH Policy and Procedures:

- auditors
- contractors

- volunteers
- Directors of the Board and
- students

Interpreters are held by the Agreement or Memorandum of Understanding that commits them to follow YourCH Policies and Procedures including this one.

5 DEFINITIONS

Term	Definition
Health information	defined in section 3 of the Health Records Act 2001 as: a) "information or opinion about i. the physical, mental or psychological health (at any time) of an individual; or ii. a disability (at any time) of an individual; or iii. an individual's expressed wishes about the future provision of health services to him or her; or iv. a health service provided, or to be provided, to an individual – that is also personal information; or b) other personal information collected to provide, or in providing, a health service, or c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or d) other personal information that is genetic information about an individual in a form which is or could be predictive of the health (at any time) of the individual or of any of his or her descendants – but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information…"
Personal information	defined in section 3 of the Health Records Act 2001 as: "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information about an individual who has been dead for more than 30 years."
Quality and safety body	a prescribed entity that has functions relating to quality and safety of health service entities (being Safer Care Victoria, being an Administrative Office within the meaning of the *Public Administration Act 2004* (Vic) and The Victorian Agency for Health Information, being an Administrative Office within the meaning of the *Public Administration Act 2004* (Vic)).
Quality and safety purpose	for the purposes of the Health Services Act 1988 and Health Services (Quality and Safety) Regulations 2020, each of the following means: • collecting and analysing information relating to the quality and safety of health service entities;

	• monitoring and review of the quality and safety of health service entities and associated risks;
	• reporting to the Secretary or to a quality and safety body in relation to the:
	  ○ performance of a health service entity; or
	  ○ risk to an individual or the community associated with the performance of a health service entity;
	• incident reporting and performance reporting in relation to health service entities;
	• incident response, including case review, in relation to health service entities.

Sensitive Information	defined as information or opinion about a person's: • Racial or ethnic origin • Political opinions • Membership of a political association • Religious beliefs or affiliations • Philosophical beliefs • Membership of a professional or trade association • Membership of a trade union • Sexual preferences or practices • Criminal record.
Service Provider	defined as the YourCH staff member providing a health service to a client.

6 RESPONSIBILITIES

Position	Responsibility
Director Capability and Impact	Holds the overall accountability and responsibility for client personal information.
Director Primary Care	is responsible for: • Ensuring that information collected through the Service Access team is collected according to the health privacy principles • Ensuring that new clients are provided with information about their rights relating to privacy and consent.
Program Managers	Responsible for: • Ensuring that clinical staff understand and comply with health privacy principles and maintain high quality client records • Receiving and reviewing incoming Health Record Access requests for their program • Consulting with relevant clinical staff regarding the release of client health records • Liaising with the Health Information Officers, relevant Director and Director Capability and Impact where the request is complex • Liaising with Health Information Officers to coordinate the release of health records when approved
Service Access Team Leader	Responsible for: • Overseeing the management of secure client information management systems and file management • Ensuring Client Services Officers provide new clients with information about their rights relating to privacy and consent.
Clinical Staff	Responsible for: • Communicating with and providing information to clients about their rights relating to privacy and consent, particularly at the first appointment • Recording any discussion about privacy in the progress notes • Obtaining and documenting consent when information is shared
Health Information Officers	Responsible for handling Health Records Access requests. The role of the Health Information Officer is to: • encompasses the duties of the privacy officer • To facilitate access to health records according to Health Records Act 2001 • To determine if there are any exceptions that apply to the release of information requested.

	• To confirm the identity of applicant or status of authorised representative • Approve release of the health information.
All staff	Responsible for: • Maintaining up to date, accurate and complete health records • Maintaining confidentiality • Participating in training • Complying with this Policy

7 RELATED DOCUMENTS

- Health Records Access form
- New Client Registration Form (Medical & Dental)
- Informed Consent Policy
- Client Identification and Procedure Matching Policy
- Code of Conduct Policy
- Client Records Policy
- Computer, Internet, Intranet and Email usage Policy
- Have Your Say Form
- Fax Cover page template
- Confidentiality and Privacy Agreements
- AMA September 2010 *Guidelines for doctors on disclosing medical records to third parties 2010 (Revised 2015)*
- DHHS December 2017 *Reporting privacy breaches to the department: Fact sheet for funded organisations*
- DHHS December 2017 *Privacy and information security guideline for funded agency staff*
- Office of the Victorian Information Commissioner (OVIC) July 2016 *Victorian Protective Data Security Standards*

8 REFERENCES AND LEGISLATION

- *Privacy and Data Protection Act 2014 (Vic)*
- *Health Records Act 2001* (Vic)
- *Health Records Regulations 2012*
- *Health Services Act 1988* (Vic)
- *Health Services (Quality and Safety) Regulations 2020* (Vic)
- *Human Services (Complex Needs) Act 2009* (Vic)
- *Child Wellbeing and Safety Act 2005* (Vic)
- *Mental Health Act 2014* (Vic)
- *Health Complaints Act 2016 (Vic)*
- *Disability Act 2006 (Vic)*
- NDIS (Protection and Disclosure of Information) Rules
- *Privacy Act 1988* (Cth) and Australian Privacy Principles (APPs)
- *Aged Care Act 1997 (Cth)*
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
- *Healthcare Identifiers Act 2010* (Cth)
- *National Health Security Act 2007* (Cth)
- *National Cancer Screening Register Act 2016* (Cth)
- *Statutory Guidelines on Research issued by the Health Services Commissioner February 2002*

9 APPENDICES

Appendix 1 – Health Privacy Principles
Appendix 2 – Australian Privacy Principles.

Accreditation Standards(s)	• QIC Standards • RACGP Standards NSQHS Standards – Public Dental (Oral Health) • Aged Care Common Standards • NDIS Quality and Safeguarding Practice Standards • DIAS • Child Safe Standards

10 Document History

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

Date	Change/ Action	Approved by
November 2013	Initial release	CEO and Leadership Team
July 2016	Review	CEO and Leadership Team
August 2017	Review	CEO and Leadership Team
March 2018	Review	CEO and Leadership Team
January 2022	Review	CEO

Appendix 1: Health Privacy Principles

Principle	Name	Description
HPP1	Collection	Health information is only collected if necessary for the performance of a function or activity and with consent. Individuals must be notified about what will be done with the information and that they can gain access to it.
HPP 2	Use and Disclosure	Health information is only used or disclosed for the primary purpose for which it was collected, or a directly related secondary purpose the person would reasonably expect. Consent is needed for any other use.
HPP 3	Data Quality	Reasonable steps are taken to ensure health information is accurate, complete, up-to-date and relevant to the functions performed.
HPP 4	Data Security and Retention	Health information is to be safeguarded against misuse, loss, unauthorised access and modification.
HPP 5	Openness	Policies on management of health information are to be clearly documented, expressed and made available to anyone who asks for them.
HPP 6	Access and Correction	Individuals have the right to seek access to health information about them, and to correct it if it is inaccurate, incomplete, misleading or not up-to-date.
HPP 7	Identifiers	A number is only assigned to a person if it is necessary to carry out functions efficiently
HPP 8	Anonymity	Individuals are to be given the option of not identifying themselves when entering transactions with organisations where this is lawful and practicable.
HPP 9	Transborder Data Flows	Health information will only be transferred out of Victoria if the organisation receiving it is subject to laws substantially similar to the Health Privacy Principles
HPP 10	Transfer/Closure of practice of health service provider	Notice must be given of transfer or closure of services to past service users
HPP 11	Making information available to another service provider	Health information relating to an individual will be made available to another health service provider if requested by the individual.

Appendix 2: Australian Privacy Principles

Principle	Name	Description
APP 1	Open and transparent management of personal information	Personal information is managed in an open and transparent way. Policies on privacy and the management of personal information must be up-to-date and available free of charge and in an appropriate form for those who request it. The organisation must be able to deal with enquiries or complaints about the APPs.
APP 2	Anonymity and pseudonymity	Individuals have the option of not identifying themselves, or using a pseudonym except for where this is impracticable for the organisation to deal with that individual
APP 3	Collection of solicited personal information	Personal information (other than sensitive information) will not be collected unless the information is necessary for the organisation to perform its functions or directly related functions and activities. Sensitive information will not be collected unless the individual consents and the information is necessary for the organisation to perform its functions, or the collection is authorised or required by Australian law or a court/tribunal order. Information will only be collected by lawful and fair means. It will be collected only about the individual and from the individual, unless otherwise consented to by the individual, required by law or order, or it is unreasonable and impractical to do so.
APP 4	Dealing with unsolicited personal information	If an organisation receives unsolicited personal information that it would not have otherwise collected, the organisation will take steps to destroy the information or ensure that it is de-identified.
APP 5	Notification of the collection of personal information	At the time of collection of personal information, or as soon as possible after, the organisation must notify the individual that the information has been collected, the purpose for which it will be used, any other organisation or body that the organisation usually discloses personal information of the kind collected, how the individual may access that personal information, and that the organisation's policy describes how a complaint about privacy can be made.
APP 6	Use or disclosure of personal information	Personal information held about an individual that was collected for a particular purpose, can only be used for that purpose unless the individual has consented to the use and disclosure, or the individual would reasonably expect the organisation to use or disclose the information for a secondary purpose.

APP 7	Direct marketing	Personal information about an individual must not be used or disclosed for the purpose of direct marketing, unless an individual would reasonably expect the organisation to disclose the information for that purpose and the organisation provides a simple means for the individual to request that they are not sent marketing information.
APP 8	Cross-border disclosure of personal information	Before an organisation discloses personal information to an overseas recipient, it must take steps to ensure that the overseas recipient does not breach APPs, unless the agency reasonably believes that the disclosure is necessary for enforcement purposes of an enforcement agency
APP 9	Adoption, use or disclosure of government related identifiers	An organisation must not adopt a government related identifier for an individual as its own identifier of an individual unless required or authorised by Australian law or it is reasonably necessary to verify the identity of the individual.
APP 10	Quality of personal information	An organisation must take such steps as are reasonable to ensure that the personal information it collects is accurate, up to date, and complete.
APP 11	Security of personal information	An organisation must take such steps as are reasonable to protect the personal information is holds about individuals from misuse, interference and loss; and from unauthorised access, modification or disclosure. Where the personal information collected by the organisation is no longer needed for use or disclosure, and the organisation is not required by an Australian law or court or tribunal order to retain the information, the organisation must take steps to destroy the information or ensure that it is otherwise de-identified.
APP 12	Access to personal information	An individual must be provided with access to their personal information on request, unless the organisation reasonably believes that providing access would pose a serious threat to the life, health or safety of the individual or the public; giving access would have unreasonable impact on the privacy of other individuals; the request is frivolous or vexatious; the information relates to existing or anticipated legal proceedings and the information would not be available through those proceedings; or giving access would be unlawful.
APP 13	Correction of personal information	If personal information held about an individual is found to be inaccurate, out-of-date, incomplete, irrelevant or misleading, or the individual requests that information be corrected, the organisation will take steps to correct that information. If that information has been previously disclosed to a third party, the organisation must take steps to notify the third party of the correction unless it is

		unlawful or impracticable to do so. If an organisation refuses to correct information it must explain that decision in writing to the individual, and the mechanisms for complaint about the refusal.