your health navigator

Healthcare Records

Status:	Current
Effective date:	May 2024
Review date:	May 2026
Approval authority:	General Manager
Responsible committee:	QRMC

Policy Intent

This policy outlines how YHN Health records are managed in order to meet the needs of clients, ensuring safe and quality care and also meet YHN's legal obligations.

Policy Statement

All YHN clients have the right to expect that their personal information is maintained in a safe, secure and confidential environment and that any medical information about them is up to date and correct and can be located and is stored for the appropriate time. Failure to meet this expectation may have a safety implication to the clients safe and appropriate care. There may also be legal implications if there is a breach of this policy and relevant and accurate medical records are not kept and stored or destroyed appropriately.

Scope

This policy applies to all YHN medical records, new, existing and both paper and electronic records. This policy applies to all YHN staff who have provide or support the provision of healthcare services to YHN clients.

Relevant Legislation

- Freedom of Information Act 1991 (*SA*)
- South Australia Health Care Act 2008
- Privacy Act 1988

Policy Overview

This policy covers the following:

- Definition of a healthcare record
- Creation of healthcare records
- Access to healthcare records
- Confidentiality of healthcare records
- Storage and security of healthcare records
- Disclosure of healthcare records
- Amendment/corrections to healthcare records
- Disposal of healthcare records
- Dealing with breaches of this policy

Definition of a Healthcare Record

A healthcare record is an official document of legal standing that supports all aspects of the care, treatment and management of clients in clinical decision making and ongoing management. The information may be both paper and electronic records.

Management of Healthcare Records

The Managing Directors of Your Health Navigator must comply with the State Records Act and its regulation in respect of healthcare records.
Adherence to NMBA professional codes and guidelines and organisational policies and procedures is included in the terms and conditions of position descriptions for all health care personnel.

Creation of Healthcare Records

Each client has one single healthcare record with a unique client identification number within the case management system – Penelope.
Main information stored on a client healthcare record is;

- Personal details
- Relevant medical history
- Assessments
- Investigations
- Diagnosis
- Treatment and support services required
- Specialist letters and correspondence
- Test results
- X-rays and scans
- Photographs
- Medications

Access to Healthcare Records

Privacy Act 1988 grants patients the right to access their medical records. Patients can access their healthcare record by written (email or paper) request to Your Health Navigator. A copy of the records or reasonable opportunity to inspect and take notes from their records will be available.

Other than exceptional circumstances permitted or required by law healthcare records will not, without the clients express up-to-date written consent, be disclosed to persons other than the client unless the client would reasonably expect such disclosure to take place, in accordance with relevant privacy legislation. For example, it is likely a client who has consented to the collection of their personal information for their healthcare may reasonably expect the health professional to share the healthcare record amongst the treating healthcare team.

For clients who are unable to provide consent due to impaired decision-making capacity, their healthcare records should not be disclosed to persons other than the clients legally appointed guardian or attorney (where appropriate) unless the guardian/attorney would reasonably expect such disclosure to take place, in accordance with relevant privacy legislation. There may be exceptional circumstances permitted or required by law.

Storage and Security of Healthcare Records

The Company will take all reasonable steps to protect the information from loss and unauthorised use or disclosure. To ensure that electronic and paper-based records are kept safe from damage, loss or theft the Compliance Standards at Appendix 1-6 will be observed including:

- Regular complete backup of the computer record by third party;
- Backup discs stored off-site in remote location by software host;

- Computers will be password protected;
- Computer passwords changed every 12 months;
- Protection against unauthorised access and amendment of records;
- Protection against computer viruses;
- Quality of resolution of scanned documents, and;
- Stored in secured cabinets.

Disclosure of Healthcare Records

All requests for client information over the phone can only be provided once the client has completed the YHN consent process at the time of referral.
YHN must establish that the caller has a legitimate and genuine entitlement to receive the information requested; and substantiate the entitlement by providing personal information pertaining to the client's record. In addition to the client's first name and family name, the caller must be able to provide other client-specific details, for example the date of birth, phone number or address which must then be verified against the client's record. Any information relating to the diagnosis of the client cannot be released.

Amendments/Corrections to Healthcare Records

Changes to electronic files in Penelope are recorded in the stdout.log file that can be retrieved and will display which user accessed/created/modified/deleted which record in Penelope.
Corrections or amendments to paper-based records will be added as a file note to patient folders.

Disposal of Healthcare Records

Healthcare records should be retained for as long as required by relevant Australian, state or territory government legislation. This means that inactive individual client healthcare records should be kept until the client has reached the age of 25 years or for a minimum of seven years from the time of last contact - whichever is the longer.

Dealing with Breaches of this Policy

Any breach must be disclosed, occurrence raised, investigated, improvement to policies and practices made. If serious may lead to Disciplinary action.

Related Documents

Your health Navigator Privacy Policy - GOV_L_0004 - Privacy Policy_v1.1
Confidentiality Policy - MGT_HR_G_0002 - Confidentiality Policy_v1.0

References

Australian Medical Association: Privacy and health Record Resource Handbook

SA Health: Health Record Management Policy Directive

Penelope – Privacy and security white paper
https://www.athenasoftware.net/wp-content/uploads/2018/03/Athena_Software_Privacy_and_Security_Whitepaper.pdf