ATMS POLICY

Record Keeping Policy – Health Records

Preamble

The health record is a foundation document which is essential for the effective and proper management of the client's healthcare needs and is the principal vehicle for communication among members of a healthcare team.

The primary purpose of the health record is to ensure that contemporaneous, accurate and relevant information on a client's care and history is maintained, to assist with ongoing treatment, and to ensure continuity of care when a client's care transfers to another health care worker, or a locum practitioner temporarily attends clinic on your behalf.

In addition, these records form an important audit tool to monitor quality of care, are valuable tools for a health care worker to use to address client concerns about their treatment and may serve as the first line of defence against any legal claim made against you. The quality of these documents often forms the focus of malpractice and negligence lawsuits, and the necessity for rigour in this area should never be underestimated.

This policy document should be read in conjunction with the Australian Privacy Principles and any other relevant federal, State or Territory privacy and health records legislation.

Health Records

The health records that you construct must be legible, factual, written in English and must be kept for at least 7 years, or where the client is under the age of 18 years at the time of treatment, records must be kept at least until that person turns 25. Your clinical notes should be written at or near the time of the consultation to which they apply, they should be exclusively clinical in nature, and contain nothing of a subjective, offensive or defamatory nature, or use abbreviations or terms that are not commonly understood.

They should be accurate and complete and should contain details such as:

- the date and time of the consultation;
- the client's name and contact details;
- the practitioner and clinic details;
- client's date of birth;
- client's healthcare insurance details;
- client's nationality;
- client's emergency contact;
- details regarding children;
- the client's usual medical adviser;
- client's medication history and current medication (including dosage);
- client's medical history;
- the client's next of kin with contact details;
- information regarding allergies or sensitivities to medications or any other substances;
- the reasons for the consultation;
- clinical findings from the consultation and your reasons for making those findings;

- medication prescribed (including the name of each individual ingredient, the amount of each ingredient used, and the dosage details) or services provided (within your scope of practice) and the reasons for providing these;
- the client's informed consent for treatment, examination and services provided. Please refer ATMS' Informed Content Policy for further information regarding informed consent.
- any warnings or cautions given to the client regarding their treatment or clinical condition;
- further treatment plan and expected outcomes;
- written copies of any advice that may be given, including copies of any referrals made for other investigations or services.
- accurate and up-to-date billing information.

The notes related to subsequent, or follow-up consultations should contain the same details that are referred to above (where relevant) and include the date of the consultation, the response to treatment and any comments by the client regarding the treatment (in their own words), details of the updated treatment plan and any further advice, as well as copies of referrals for any further investigations or services. Any unexpected outcomes that occur because of your treatment or adverse reactions to that treatment should also be recorded and where appropriate, and adverse reactions to ingested medicines (where provided within your scope of practice), or services provided, or therapeutic devices, must be reported to the Therapeutic Goods Administration.

Security

Health records should be stored securely, and accessible only by staff members on a need-to-know basis (i.e. those involved in treating the client, and administrative staff handling records). Where electronic files are used, the files must be password protected, those passwords made known only appropriate staff, the files backed up and those file copies stored securely offsite. Passwords must be strong and changed regularly. Practitioners are encouraged to share passwords securely via password protection software such as 1password. Passwords should be changed when staff leave the employ of the clinic. Where hard copies of files are used, they must be held securely (i.e. in locked cabinets/rooms in alarm protected buildings) and not subject to unauthorised access.

Destruction of Health Records

Files that are no longer legally required to be kept should, in the case of electronic files, be securely and completely deleted as should all copies of those files, and hard copies should be securely shredded or incinerated under supervision with consideration to the environmental impact of these processes and steps should be taken to minimise that impact. It is advisable to engage commercial service provider who is experienced in carrying out the destruction of confidential information. Once the destruction is complete, you should keep a record or receipt of the destruction and include the following:

- name of the person that the medical record related to;
- period of the health record (i.e. the date of the first entry through to the date of the last entry); and
- date that the record was destroyed.

Anti-virus Software and Cyber Insurance

Anti-virus software should be installed on all computers and such software kept up-to-date. Staff should be trained on how to use the software and their responsibilities for ensuring it works effectively. Firewalls should also be installed to protect your system against unauthorised access however these may be included as part of your anti-virus software. Anti-spyware software is also recommended.

ATMS recommends practitioners maintain a cyber insurance policy to protect against cyber-attacks.

Privacy
Health records, including the client's personal information or images, must not be transmitted in any way, shared or reproduced, even if the person is not directly named or identified, without the written and informed consent of the client. If you relocate or close your clinic, you must facilitate arrangements for the transfer or management of all these records in accordance with the Australian Privacy Principles and all other relevant legislation governing privacy and health records.

Access to Health Records
Except where one or more elements of section 6.1 of the Australian Privacy Principles can be demonstrated, should a client, their legal representative, their private health insurer, or an organisation legally mandated to do so, request a copy of the client's health record, you must promptly comply with that request.

Other related policies:

ATMS Informed Consent Policy
ATMS Receipts Guideline
ATMS Online Audio-Visual Consultation Policy
ATMS Dispensing Policy