Chinese Medicine Council of New Zealand

Clinical Records Guidance

Introduction

The Chinese Medicine Council of New Zealand (the Council) is legally required to set standards of clinical competence, cultural competence, and professional conduct to be observed by all registered Chinese medicine (CM) practitioners. The Council has established a standards framework which defines ethical and professional standards, and practice standards that all registrants must meet.

The standards set by the Council are minimum standards that are used by the Council, the public of New Zealand, competence review committees, professional conduct committees, the Health and Disability Commissioner, the Health Practitioners Disciplinary Tribunal, and the courts, to measure the competence, performance and conduct of practitioners. A failure to adhere to the Council's standards may result in Council involvement and may impact on a practitioner's registration.

This document supplements and expands on the Clinical Records Standard available on the Council website.

Purpose

Chinese Medicine (CM) practitioners have a responsibility to ensure safe practice and the interests of tangata whai ora, firstly by maintaining accurate, time-bound, and up-to-date clinical records and secondly by protecting the confidentiality of health information. It is vital that practitioners maintain the trust of tangata whai ora by treating all health information as sensitive, private, and confidential.

Legislative context

CM practitioners must be familiar with the law governing this area of practice including but not limited to:

- The Health Information Privacy Code 2020
- The Health (Retention of Health Information) Regulations 1996
- The Code of Health and Disability Services Consumers' Rights

The Code of Health and Disability Services Consumers' Rights guarantees every consumer the right to have quality services provided with reasonable care and skill that complies with legal, professional, equitable, and other relevant standards. This includes documenting and managing health information appropriately.

The Privacy Act 2020 applies to any action taken, and all personal information collected or held by a New Zealand entity, both inside and outside New Zealand; and to any action and all personal information collected or held by an overseas entity in the course of "carrying on business" in New Zealand.

Where the information concerns the health of tangata whai ora, the Health Information Privacy Code 2020 (HIPC) also applies and has the same legal standing as the Privacy Act.

The New Zealand Standard Health Records (NZS 8153:2002) sets out the minimum requirements for the appropriate documentation and management of health records within public and private healthcare services in New Zealand.

"On the record. A practical guide to health information privacy", published by the Office of the Privacy Commissioner, is a useful additional reference for CM practitioners.

Content of clinical records

CM practitioners must create and maintain clinical records that are comprehensive, time-bound, and up to date; and that represent an accurate and complete record of the care provided.

Clinical records must be kept in a document or file specific to that individual and contain the following:

- Key demographic data: full name, NHI number (if available), date of birth, gender, ethnicity, contact details, and, where needed, residency status and name of the Primary Health Provider
- Emergency contact
- The date (and in some instances time)
- The presenting complaints
- The principal/primary diagnosis
- Relevant associated conditions or additional diagnoses
- Relevant family or personal history
- Medications
- A comprehensive subjective and objective assessment
- Analysis of clinical signs and symptoms
- Relevant outcome measurements
- Treatment goals and management plan
- Information given to tangata whai ora
- A record of a signed consent form or refusal
- Treatment provided including (if acupuncture) details of treatment; retention; other techniques; herbal formula/prescriptions (for more detail refer to guidance section on 'Safe prescribing of herbal medicines')
- The dates of all treatment/s, referrals, and any other interventions;
- Progress made and discharge plan
- Letters and reports to, or from, referring health professionals or other involved parties, and any clinical photographs and/or digital images. These need to be dated
- Note of risks and/or problems that have arisen and the action taken to rectify them, and
- Electronic authentication or printed name, signature, and designation of the CM practitioner responsible.

General guidelines

1. Tangata whai ora should feel confident that their health information will be recorded respectfully, with their appropriate informed consent regarding their cultural needs (see Council's Informed Consent Standard) and be kept confidential (except where sharing is legally required)
2. Practitioners must understand that tangata whai ora, or authorised third parties, may read the information in the clinical records they create and therefore documentation should be accurate and respectful. Care should be taken to consider the impact on tangata whai ora if they were to read the information written
3. Clinical records should both document the information that was provided to tangata whai ora and whether, or not, informed consent was given

4. Practitioners must take reasonable steps to correct the health information of tangata whai ora, upon their request. A corrected note and date must be recorded in their health information when requested
5. Clinical records should be in English or Te Reo Māori, on a permanent electronic record or, if on paper, be legible and in pen
6. Where records are maintained in a language other than English, on occasion it may be necessary to provide translated information to a third party, it should be translated by a certified translator or by a practitioner with no conflict of interest. The cost of such translations must be borne by the practitioner
7. Clinical records should be made for each consultation, at the time of the consultation.
8. Clinical records should be recorded in such a way that another practitioner (CM and other healthcare) can easily understand the treatment provided and rationale behind it to allow for transfer and continuity of, care
9. Clinical records should meet the Council's Professional Standards and be able to withstand scrutiny by the Council and its representatives; the practitioner's professional body; peer review; audit; or a medicolegal challenge
10. Clinical records should utilise outcome measures when appropriate
11. Practitioners should respond to, adequately document, and report adverse events, and
12. Practitioners must not delete information entered in the clinical record at an earlier date. If any changes are made the practitioner must ensure their name, and the date of entry, are entered alongside any correction or other changes.

Third party requirements

When working for third parties, such as ACC (Accident Compensation Corporation), it is important that CM practitioners are aware of and adhere to all clinical note requirements specific to that entity.

ACC requires that the services provided and invoiced for must be supported by clinical records that meet both ACC requirements and the standards set by the Council.

Safe prescribing of herbal medicines

For more detail on this refer to the Council's Safe Practice Standard

The Council recommends registered practitioners write clinical records in English (or in pinyin for the herbal formulae name) and on prescriptions and labels. Where records are maintained in a language other than English, on occasion it may be necessary to provide translated information to a third party, it should be translated by a certified translator or by a practitioner with no conflict of interest.

CM Practitioners should:

- To use clear and consistent herbal nomenclature
- To record appropriate and complete details of Chinese herbal medicines and dosages in clinical records
- Write appropriate prescriptions that are fit for purpose. Prescriptions are to be printed or handwritten clearly and legibly, in easily understood English. Herb names are to be in *pinyin* in accordance with the Chinese Medicine Board of Australia's Nomenclature Compendium of commonly used Chinese herbal medicines
- To ensure medicine labelling is accurate and informative, and

- To ensure compounding and dispensing of medicines is competent, precise, and professional.

When prescribing raw herbs and herbal extracts, the following information must also be included, in English if requested by tangata whai ora. The same information can also be provided in another language, if English is not the first lanagauge of tangata whai ora, to promote compliance and safety:

- Name of tangata whai ora (given name and family name) or parent, guardian, or agent/representative (when applicable)
- The name, registration number and contact telephone number of the prescribing CM herbalist and their signature
- Date prescribed (day/month/year)
- Names of the herbs in *pinyin* and amounts of each herb (measured in grams)
- Type of processing (when relevant)
- Specific directions for use (dose, preparation/cooking, route of administration, frequency, timing of consumption)
- Number of packets (where relevant)
- The expiry date of the prescription (i.e., date 'not to be dispensed after'), and
- Specific warnings[1] (when appropriate).

Security of Health information

Physical security

Protect the physical security of health information and clinical records by:

- Physically securing and restricting access to the areas in which information is stored. Take simple precautions such as locking filing cabinets and locking unattended rooms and do not store records in your clinic rooms
- Positioning computer screens so that they cannot be seen by unauthorised persons
- Using security screen saver programmes to prevent unauthorised persons from seeing computer screens and using automatic log-off of computer systems after a set period of non-use
- Protecting physical clinical records from hazards, for example, fire
- Storing records that are not being used for current or regular care, but that need to be legally held, in a safe and secure manner that protects their security.

Operational security

Protect the operational security of health information and clinical records by:

- Keeping health information confidential
- Disclosing health information only to tangata whai ora, or their representatives, unless an exception applies
- Not accessing the health information of tangata whai ora you have not provided care for, when using a shred system, unless an exception for the use or disclosure of health information applies
- Ensuring team members understand their obligations in relation to the confidentiality and privacy of health information

[1] Warnings on keeping out of reach of children may be required for example when even a small quantity if ingested could be toxic or where a choking hazard occurs due to the size of parts of herbs. Such warnings are to be legible and prominent

- Understanding that health information cannot be discussed with anyone other than team members who already hold this information, unless an exception applies
- Holding any discussion/s involving health information in private areas of the practice, where practical, not in shared spaces such as the waiting room, reception area, or staff room
- Avoiding the collection of health information verbally in public waiting areas, where discussions can be overheard
- Keeping health information on the premises where possible, and keeping information secure when there is a need for it to be off-site; for example, storing 'archived' clinical records off-site, except in the case of health information stored in cloud services
- Making health information anonymous when it is being used for education purposes, and using fictitious information when training individuals in the use of systems
- Withholding, as far as practical, access to health information from IT services personnel
- Maintaining a list of team members who are authorised to use the IT system
- Managing authorised users' access consistent with their role, so that access to health information is on a 'need-to-know' basis
- Using password vaults is strongly recommended, and
- Providing training for team members on the proper use of the computer system, which includes the protection, security, and privacy of health information.

Technical security

When selecting and maintaining a computer system for the collection of health information:

- SaaS clinical record keeping systems are now recommended by Te Whatu Ora. A hosted service provider owns and oversees the infrastructure, software and administrative tasks and makes the service available to clients, so that there is no need to maintain additional hardware and software. Practitioners, however, are responsible for the security and integrity of personal health information that is stored or processed by public cloud services
- All practitioners wanting to store personal health information in a public cloud service must ensure that the provider is explicitly HIPAA compliant, GDPR compliant, and /or meets the requirements of the NZ Health Framework
- Use only software designed for recording, processing, storing, and retrieving health information, and
- Set up security, firewalls, and anti-malware systems to protect health information from direct unauthorised access, and unauthorised access through hacking or invasion of hostile or intrusive software.

Sharing information

CM practitioners should consider developing a practice procedure for sending out health information that reflects the guidance below:

For email	• Consider the nature of the information to be sent, who the intended recipient is, and whether email is the most appropriate form of communication. If the email recipients are tangata whai ora, confirm that you have their permission to communicate with them in this way; • Ensure email addresses are accurate and current;

	• Do not use lengthy 'chains' of responses in emails, as sensitive information may be unwittingly included by an earlier response; • Limit the number of "cc" addresses to only those who are authorised to receive the information.
For post	• Ensure the type of physical delivery is appropriate for the nature of the information (general post, registered post, couriered post, track-and-trace, and hand delivered post); • Ensure addresses are accurate and current before posting; • Ensure postal items are kept secure until lodged.
For text messaging	• Check you have consent to send them text messages; for example, appointment reminders. Record consent or refusal in the health record; • Do not include clinical information in text messages.

Retention and disposal of clinical records

- All health records must be retained for a minimum of 10 years from the day following the last dated clinical consultation
- Retention of records for longer than the minimum 10 years is recommended for children with significant problems or tangata whai ora with ongoing conditions likely to persist long-term
- Disposal of documents must ensure their confidentiality. Destroy physical records by controlled incineration or shredding, ensuring that no information is lost or removed during the process and that the resulting waste does not include fragments of readable personal information. Alternatively, a reputable document destruction company can be used
- Destroy computerised records by using an appropriate electronic or physical process to ensure the record is unreadable. Simple deletion from the device may be inadequate as data recovery is possible. Seek expert advice if you are unsure, and
- Privacy and security requirements must be met, and everything necessary and practicable must be done to ensure that the destruction of records is complete.

Privacy breaches

A privacy breach occurs when an organisation or individual either intentionally or accidentally:

- Provides unauthorised or accidental access to someone's personal information
- Discloses, alters, loses, or destroys someone's personal information, and
- When someone is unable to access their personal information due to, for example, their account being hacked.

Under the Privacy Act 2020, if any organisation or business that has a privacy breach that will cause, or is likely to cause, anyone serious harm, must notify the Privacy Commissioner and any affected people as soon as practically possible. Act promptly to manage an actual or suspected breach of health information.

The Privacy Commissioner has an online tool NotifyUs that is available to assist in determining if a breach is notifiable and to guide practitioners through the notification process.

Acknowledgements

This document incorporates and acknowledges information from Accident Compensation Corporation, Acupuncture New Zealand, the Dental Council of New Zealand, New Zealand Acupuncture Standards Authority, the Osteopathic Council of New Zealand, and the Physiotherapy Board of New Zealand.

The Council also acknowledges the input from Scott Pearson (Clinical software founder).