Australian Institute of Kinesiologists Ltd

Client Data Collection and Storage Policy

Updated 3 September 2020

Preamble

As Kinesiologists, we are responsible under Australian law for keeping accurate and complete client records. This includes the safe collection and secure storage of our clients' data. This is essential for the effective and proper management of our clients' health care needs.

You are required to keep client records that are accurate, complete, and securely stored, to:

- protect client privacy;
- ensure that client trust in you as a Kinesiologist and health care professional is maintained;
- assist if you need to refer your client to another health practitioner; and
- protect you in the event of any allegations of negligence or other legal action that may be brought against you.

Purpose

This policy provides a minimum set of standards you must abide by when collecting and storing client data.

You should read and consider this policy in conjunction with the current AIK Ltd's **Code of Ethics and Conduct**. You should also refer to your state and federal laws on data record-keeping, data privacy/confidentiality and data protection/security.

Scope of policy

This policy covers all aspects of collecting and storing client data, including, *but not limited to*:

- client personal information;
- health assessments;
- case histories;
- referrals;
- appointment bookings;
- consultation records; and
- related data held in paper or electronic formats.

Data collection

The client data you collect should be accurate and complete, and should contain details such as (but not limited to):

- the date of the consultation;
- the client's name and contact details;
- the client's date of birth;
- the client's healthcare insurance details;
- the client's emergency contact/s;
- the client's usual medical adviser;
- the client's medical history and medication history;
- the client's next of kin with contact details;
- any information regarding allergies or sensitivities to medications or any other substances;
- reasons for the consultation;
- record of their written signed consent to the session; and
- any findings from the balance undertaken in the session.

Your clinical notes should be written at or near the time of the consultation to which they apply. They should be factual in nature, and not contain anything that is subjective, offensive or defamatory in nature. They should also not have abbreviations or terms that are not commonly understood.

Data storage and security

Your client records must be stored securely, and accessible only by you and any authorised staff you may have (such as a receptionist).

Paper records

- You must keep paper records in a locked cabinet (or other secure system) that cannot be accessed by anyone who does not require access.
- If you remove or move records (for example, to take to a home visit), they should be stored in a secure, locked container and kept out of sight while in transit.
- You must use paper that is not able to be easily damaged or degraded. The use of loose notes (e.g. sticky notes) is strongly discouraged.

Electronic records

- You must store any electronic client records in a password-protected system that cannot be accessed by anyone who does not require access.
- You should also ensure that you change passwords to access the data on a regular basis (e.g. monthly).
- It is recommended that you consider taking out a cyber insurance policy if you are storing your client records electronically. As you are usually storing information on your clients of a private and sensitive nature (such as their name, address and medical records), cyber insurance covers you if your computer systems get hacked and the data on those systems is unlawfully accessed or stolen.

Electronic storage systems

Electronic Digital Records Management Systems (EDRMS)

If you choose to store your client data electronically, an Electronic Digital Records Management System (EDRMS) is recommended, rather than a standard computer folder system. An EDRMS has built-in features that facilitate better management and more secure storage of data. You are encouraged to do your own research to find out which systems would be suitable for your use.

Cloud storage over the internet

Cloud storage allows you to store documents such as client records over the internet, which is designed for convenience, but you need to be careful with the security of such facilities when it comes to keeping your clients' data safe.

You are advised to not use unsecured cloud services, such as Google Drive, Microsoft One Drive and Dropbox. This is because these services usually store the data you put into them in locations overseas, which would mean that the data would not be subject to the same legal protections as data stored in Australian-based services.

The Australian Cyber Security Centre website provides more information on the use of cloud services and cyber security more generally.

Digitalisation of paper records

- If you choose to digitise your client records, the entire client record must be digitised. Once you complete this process, you must check to ensure that the records remain complete and accurate in the digited form. Evidence of this check being done must be included with the record.
- The digitised records must restrict or prevent any changes or alterations to be made to the records. If you need to make changes to these records, you need to keep a record of those changes, or clearly mark them on the records that were changed.

Backup of electronic data

- You must have a Disaster Recovery and/or Business Continuity Plan in place for any electronic system storing client data. This is required for you to manage any risks if your electronic client system is damaged or compromised. For example, your system's data must be regularly backed up onto other storage systems.
- When you back up your data, if it is stored internally (i.e. in the same place as where you store your original data), you need to take into account that if a disaster occurs at that place, you could potentially lose both your original and back-up copies of your clients' data.
- If you back up and store your data off-site, the location must be somewhere in Australia. If you choose to back up your data using a cloud service, please ensure you adhere to the policies stated earlier on cloud storage.

- You need to have appropriate security on your back-up systems at the same level of security as (or better than) your main client data storage system. It should restrict access to that data by secure passwords or other secure means.

Access to client records

A client may, under Australian law, request access to the personal information that you keep as part of their client record. Access can be given by providing a copy of their record, or by allowing the client to view their record.

Retention of client records

- You are required to retain client records for a minimum of seven (7) years from the date of the last amendment to the client record. The date of last amendment is date of the last service provided to the client, the date of the last contact with the client, or the date you are notified that the client is deceased. This is known as the 'minimum retention period'.
- You must not destroy a client record where any of the documents are within the minimum retention period.
- You cannot destroy part of a client record - the record must remain complete for the entire minimum retention period.
- After seven years from the date of the last amendment to the client's record, you may retain or destroy the record, noting the following:
    - Electronic files should be completely deleted, including any back-up copies of those files.
    - Paper copies should be shredded or incinerated under supervision with consideration to the environmental impact of these processes.