1. PURPOSE OF POLICY

In accordance with the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012 (including the Australian Privacy Principles (APPs), in conjunction with all relevant state and territory privacy legislation, Birkita Pty Ltd TA Momentum4 has established standards for the management of personal and health information.

These standards set out our obligations in relation to the collection, retention, security, access, use and disclosure of personal and health information. In the course of providing our services, there is certain personal information we may require.

Who is responsible for privacy?
It is the responsibility of all Momentum4 employees and contractors to protect the privacy of any individuals by managing personal and health information in accordance with this policy.

What is personal information?
Personal information is any information or opinion about an identifiable person ("an individual"). This includes records containing an individual's name, address, telephone number and gender.

What is health information?
Health information is a specific type of personal information, which includes information or an opinion about the physical or mental health of an individual, or the disability of an individual.

2. PRIVACY STANDARDS

2.1 Collection

- Lawful – Momentum4 will only collect personal and health information directly related to a function or activity related to the function or activity being offered.
- Relevant – Momentum4 will ensure that the health information collected is necessary, relevant, accurate, complete and up to date.
- Direct – Momentum4 will collect personal and health information directly for an individual whom the information relates to unless; the individual has authorised collection of the information from someone else, or in the case of information relating to a person under the age of 16 years, the information has been provided by a parent or guardian of the person.
- Open – Momentum4 will take reasonable steps to inform individuals (and their representatives) why we are collecting information, what we will do with it and who will see it.

2.2 Storage and Protection

- Storage – Momentum4 records of individuals information are kept in electronic form, when not required for clinical care.
- Momentum4 is required by law to retain medical records for a period of seven years.
- Protection – Electronic information kept on computers is password protected and is available only to Momentum4 employees and contractors who are involved in managing an individual, in the course of the Momentum4 business.
- Disposal – Information or hard copy documents that are no longer required are disposed of appropriately using shredding machines into secure bins. Electronic data (where appropriate, with

exceptions as aforementioned) is securely deleted so it is no longer accessible.

2.3 Access and Accuracy

- Transparent, Accessible and Accurate – Momentum4 will take all reasonable steps to explain what personal and health information we are storing and how an individual is able to access this information without unreasonable delay or expense. Momentum4 will endeavour to ensure that the information is relevant, up to date, complete and accurate before using it.

2.4 Use and Disclosure

- Limited – Momentum4 will only use and disclose an individuals' health information for the purpose for which it was collected, where the individual concerned is aware of through explicit consent and it is a directly related purpose that you would expect. Momentum4 does not expect to disclose personal information to any overseas recipients. Momentum4 does not use or disclose personal information for the purpose of direct marketing. However, the organisation may use personal or health information without consent in order to deal with a serious and imminent threat to any person's health or safety, where illegal activity is suspected or where requested by law enforcement authorities.

2.5 Identifiers

- Identification – Momentum4 allocates unique case numbers to all clients for internal use only, in order to effectively manage case records including file notes, reports and case records.

2.6 Information Collected

The amount and type of personal information Momentum4 collects and holds about an individual referred to us may, but not be limited to include:

- Personal details such as name, address, date of birth, and contact details including telephone numbers, address and photo ID.
- Information about a medical condition, and the nature of the condition and the manner in which any injury or condition arose.
- Functional and psychological status in relation to the compensable injury or condition (compensable under a government or private insurance scheme) and any other medical factors that may be disclosed that may impact on functional or psychological capacity, recovery and/or return to work.
- Information regarding employment, wage histories and compensation benefits where relevant.
- Information regarding social and work relationships as and when applicable to the purpose for which we are engaged.
- Information collected is relevant to the purpose, not excessive, is accurate and up to date.
- Information does not intrude to unreasonable extent on the personal affairs of the individual to whom the information relates to.

2.7 How is the information collected?

- Via telephone, video conference, correspondence and liaison.
- Face to face during assessments or meetings.

- Through any photographic, auditory or video recordings.
- Via Telehealth for the purposes of assessments, treatment or counselling sessions and meetings.
- Through medical case conferences.
- At the workplace through assessment or meetings.
- Through the reports of third parties including treatment providers.
- Through medical reports and investigations that are provided by other parties as required for eligibility of benefits within the Workers Compensation Scheme.

2.8 Purpose of collecting and holding information?

- To ensure the most efficient and useful direction of services.

2.9 Anonymity and Pseudonymity

Individuals have the option of not identifying themselves or of using a pseudonym unless the Momentum4 is required or authorised under Australian law or a court/tribunal to identify the individual or it is impracticable to deal with the individual anonymously or by a pseudonym.

2.10 Overseas recipients

No personal data is provided to overseas recipients.

3. CONSENT

Consent is provided by one or more of the following means.

- By completing and signing the Momentum4 consent form. This includes during direct face to face contact or through Telehealth platforms and electronic applications.
- By obtaining verbal approval from the individual for the release and exchange of information to relevant scheme participants. In this instance a clear file note is documented.

Where an interpreter is involved, Momentum4 ensures that the interpreter co-signs any information release agreement.

In relation to the Momentum4 service provision, information may be exchanged between the nominated treating doctor, the employer, the insurer or agent, other treating practitioners, injury management consultants and any other authorised scheme authority or administrator.

Third Parties

Where reasonable and practicable to do so, we will collect your personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

4. INFORMATION AND DOCUMENT ACCESS

All requests for personal information must be sent in writing to Momentum4 by emailing admin@Momentum4.com.au. Momentum4 endeavours to respond within a reasonable period

after the request is made and provide access to the information in the manner requested where reasonable and practicable to do so.

Any request for the release of an individuals' information is to be forwarded to the Senior Clinical Officer for processing.

Momentum4 will provide an individual with copies of all assessments, plans or reports prepared for them, unless it is deemed that information contained within those reports may be detrimental to the health and welfare of the individual. This may be particularly relevant for individuals with psychological injuries. Further, note that there may be other grounds on which information may not be disclosed including where it is unlawful to give access to the information or to the extent that giving access would have an unreasonable impact on the privacy of other individuals. If access to personal information is refused, or access in the manner requested is refused, Momentum4 will write to the individual to inform them of the reasons why (unless unreasonable to give reasons having regard to the grounds of refusal) and the complaints process.

Momentum4 will not provide an individual's or any other party, reports received from third parties. The individual will be advised that requests for such information need to be forwarded to the relevant author of the report or the third party in question.

Momentum4 may also provide information to other parties in the case where:

- We reasonably believe it is necessary to assist an enforcement body to perform its functions.
- We suspect that an unlawful activity has been, is being or may be engaged in and the personal information is a necessary part of our investigation or reporting of the matter.
- We reasonably believe it is necessary to prevent a threat to life, health or safety.
- We are authorised or required by law to do so, (e.g. where information is required by bodies regulating us or in response to subpoenas or warrants).
- We have contracted an external organisation to provide support services and that organisation has agreed to conform to our privacy standards

5. FILE AND INFORMATION CONSISTENCY

To ensure correct information and data collected from individuals is consistent across the board, Momentum4 employees and contractors are trained and mentored as to keeping accurate file notes.

File reviews and supervision between the mentor / supervisor and employee will provide feedback to Momentum4 employees and contractors as to how to effectively obtain and update important information from an individual and record this in a consistent manner whilst maintaining respect and confidentiality at all times.

Where Momentum4 is satisfied personal information held is inaccurate, out of date, incomplete, irrelevant or misleading, or where an individual requests that Momentum4 correct information, we will take reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading having regard to the purpose for which the information is held. Where, an individual requests that other entities using that information are notified of any correction of information, Momentum4 will take reasonable steps to do so unless it is unlawful or impracticable to do so.

Where Momentum4 refuses to correct the information, Momentum4 will write to the individual to inform them of the reasons why to the extent reasonable to do so and the complaints process. Where an individual requests that a statement is associated with the information that the individual considers

that the information is inaccurate, out of date, incomplete, irrelevant or misleading to make their view apparent to users of that information, Momentum4 will take reasonable steps to do so

6. PRIVACY ON OUR WEBSITES AND APPLICATIONS

This policy also applies to any personal information Momentum4 collects via its websites, and applications, including mobile applications, in addition to personal information individuals provide to Momentum4 directly, through completing request forms or registration forms.

Use of cookies

Cookies are pieces of information that a website transfers to a computer's hard disk for record-keeping purposes. Most web browsers are set to accept cookies. Cookies, of themselves, do not personally identify users, although they do identify a user's browser and where a site visitor has voluntarily provided personal information about themselves subsequent visits can be tied to this information. Cookies allow Momentum4 to record how many people are using different parts of the website. It is possible to set the browser to refuse Cookies, however this may limit the services provided by the Momentum4 website.

Communication

Momentum4 may contact an individual using the personal information provided in order to:

- Keep the individual informed of latest trends within the workplace wellbeing sector and provide relevant workplace health information.
- Provide information about upcoming events and other matters that may be of interest.
- Send newsletters and updates on services and changes including relevant legislative requirements.

If an individual receives any communications from Momentum4 which they no longer wish to receive, they may request removal of their personal information from the mailing list by emailing admin@Momentum4.com.au, allowing 21 days for this request to be processed.

7. PRIVACY COMPLAINTS

Grievances concerning team member or individual privacy (including concerning potential breach of the Australian Privacy Principles) should be raised in the first instance with the team members Manager. If this Manager is unable to resolve the matter, it may be referred to the CEO by emailing admin@Momentum4.com.au

Should the individual feel their complaint has not been resolved at this level, or after 30 days of making the initial complaint, they may then complain to the Office of the Australian Information Commissioner.

8. DATA BREACH RESPONSE

As per the *Privacy Act 1998*, Momentum4 have an obligation to report privacy breaches. As a result of an amendment to the *Privacy Act: Privacy Amendment (Notifiable Data Breaches) Act 2017*, notification to the Office of the Australian Information Commissioner (OAIC) will be mandatory when a data breach could give rise to a 'real risk of serious harm' to the affected individuals.

When to report a data breach

Under the Notifiable Data Breach (NDB) scheme an organisation or agency must notify affected individuals and the OAIC about an eligible data breach.

An eligible data breach occurs when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an organisation or agency holds
- this is likely to result in serious harm to one or more individuals, and
- the organisation or agency hasn't been able to prevent the likely risk of serious harm with remedial action

An organisation or agency that suspects an eligible data breach may have occurred must quickly assess the incident to determine if it is likely to result in serious harm to any individual.

Further information on this can be found at:

https://www.oaic.gov.au/privacy-law/rights-and-responsibilities

https://www.oaic.gov.au/privacy/privacy-complaints/

Information about the Australian Privacy Principles can be found at: https://www.oaic.gov.au/privacy/australian-privacy-principles/