HEALTHGUARD FIRST AID
TRAINING SERVICES

Privacy Policy

POLICIES AND PROCEDURES

First aid, not pretty aid!

1. PURPOSE

To purpose of this Privacy Policy is to outline how Healthguard maintains compliance with relevant legislative requirements and make this information available to staff, individuals and other third parties with whom Healthguard interacts.

2. POLICY STATEMENT

Healthguard is committed to maintaining the privacy and confidentiality of its clients and staff records. Healthguard complies with the Privacy Act 1988 including Australian Privacy Principles as found in the Privacy Amendment (Enhancing Privacy Protection) Act 2012. Healthguard manages personal information in an open and transparent way and provides staff with suitable procedures to manage related inquiries and complaints.

3. SCOPE OF POLICY

This policy applies to all staff, individuals and third parties with whom Healthguard interacts and where personal information is collected, retained, used or shared.

4. POLICY PRINCIPLES

4.1 MANAGING PERSONAL INFORMATION

4.1.1 Purposes for information collection, retention, use and disclosure

Healthguard retains a record of personal information about all individuals with whom we undertake any form of business activity. There are certain reasons why we must collect, hold, use and disclose information, e.g:

- providing services to clients
- managing staff and contractors and third party providers
- promoting products and services
- conducting internal business functions and activities.

Healthguard may disclose information held on individuals for valid purposes to a range of entities including governments (Commonwealth, State or Local); and employers (and their representatives).

4.1.2 Kinds of personal information collected and held

The following types of personal information are collected, depending on the need for service delivery:

- contact details
- employment details
- product/service progress and achievement information
- financial billing information.

The following types of sensitive information may also be collected and held:

- identity details
- complaint or issue information.

4.1.3 Collection of personal information

Where possible Healthguard prefers to collect required personal information directly from the individuals concerned. This may include the use of forms (such as enrolment forms) and the use of web based systems (such as online enquiry forms, web portals or internal operating systems).

Healthguard may receive some information via third party sources in undertaking service delivery activities. This may include information from governments (Commonwealth, State or Local), employers and their representatives, co-providers with whom we have a Third Party Agreement.

4.1.4 Storage of personal information

Healthguard's usual approach includes suitable measures to ensure personal information is held securely. Where possible, information is:

- stored electronically (if paper based, converted to electronic means as soon as practical)

- stored in secure, password protected systems, such as financial and student management system
- monitored for appropriate authorised use at all times.

Only authorised personnel are provided with login information to each system, with system access limited to only those relevant to their specific role. Healthguard ICT systems are virus protected, backed up and access is monitored. Individual information held across systems is linked through Healthguard allocated identification number for each individual.

4.1.5 Retention and destruction of information

Healthguard has a Records Management Policy which details the periods for which personal information records must be kept. Destruction of paper based records occurs as allowable by electronic storage and our Records Management Policy. Documents are destroyed appropriately and securely.

4.1.6 Accessing and seeking correction of personal information

Healthguard confirms all individuals have a right to request access to their personal information held and to request its correction at any time. A number of third parties, other than the individual, may also request access to an individual's personal information.

Individuals or third parties may at any stage request that their records held by Healthguard relating to their personal information be updated. Upon this request, Healthguard will correct personal information held and notify any third parties of corrections made to personal information, if this information was previously provided. The procedure to access and correct personal information is detailed at the end of this policy.

4.1.7 Healthguard initiated correction of personal information

Healthguard takes reasonable steps to correct personal information we hold in cases where we believe the personal information held is inaccurate, out-of-date, incomplete, irrelevant or misleading. This awareness may occur through collection of updated information, in notification from third parties or through other means.

4.1.8 Complaints about a breach of privacy

If an individual feels that Healthguard may have breached their privacy or this policy, the procedure to complain is detailed at the end of this policy.

4.1.9 Likely overseas disclosures

Healthguard confirms that individuals' personal information will not be disclosed to overseas recipients other than in the course of general cloud hosting requirements of the Healthguard Student Management System or other cloud storage solutions. Varied overseas locations may be used as part of reputable cloud hosting services for provision of portal services.

4.1.10 Availability of Privacy Policy

Healthguard provides this Privacy Policy from the Privacy link on our website at www.healthguardfirstaid.com.au/course-and-participant-information and If reasonably practical, this Privacy Policy can also be made available in a different format as requested by the individual.

4.1.11 Review and Update of this Privacy Policy

Healthguard reviews this Privacy Policy on an ongoing basis, as part of continuous improvement, or as government required changes are identified. Where this policy is updated, changes to the policy are communicated to staff and published to the Healthguard website.

4.2 OFFERING ANONYMITY OR PSEUDONYMITY

Healthguard does not require a person to identify themselves when dealing with us unless it is necessary for the individuals' information to be collected to complete a request. For example, a person can send an email enquiry to Healthguard without providing their name, however they will need to provide their legal name to enrol in a course, or provide a name for billing details when purchasing items.

If there is an option to deal anonymously or by pseudonym with us, individuals will be told of this option. For example, student user names for our learning system are email addresses that do not need to include an individual name or identifying information.

Healthguard only stores and links pseudonyms to individual personal information in cases where this is required for service delivery (such as system login information) or once the individual's consent has been received.

4.3 COLLECTING PERSONAL INFORMATION

4.3.1 Collection of solicited personal information

Healthguard only collects personal information that is reasonably necessary for our business activities. We only collect sensitive information in cases where the individual consents to the sensitive information being collected, except in cases where we are required to collect this information by law. All information we collect is collected by lawful and fair means. We only collect solicited information directly from the individual concerned, unless it is unreasonable or impracticable for the personal information to only be collected in this manner.

4.3.2 Dealing with unsolicited personal information

Healthguard may occasionally receive unsolicited personal information. If it is information that we would not have collected lawfully or for a valid business purpose we will immediately destroy or de-identify the information (unless it would be unlawful to do so).

4.3.3 Notifying individuals of the collection of personal information

When Healthguard collects personal information about an individual, we take reasonable steps to notify the individual this has occurred. This includes:

- Showing Healthguard's contact details, including the position title, telephone number and email address of a contact who handles enquiries and requests relating to privacy matters
- the facts and circumstances of collection such as the date, time, place and method of collection, and whether the information was collected from a third party, including the name of that party
- if the collection is required or authorised by law, including the name of the Australian law or other legal agreement requiring the collection
- the purpose of collection, including any primary and secondary purposes
- the consequences for the individual if all or some personal information is not collected
- other parties to which the information is usually disclosed, including naming those parties
- whether we are likely to disclose the personal information to overseas recipients, and if so, the names of the recipients and the countries in which such recipients are located
- a link to this Privacy Policy on our website
- advice that this Privacy Policy contains information about how the individual may access and seek correction of the personal information held by us, how to complain about a breach of the policy, and how we will deal with such a complaint

Where possible, we ensure that the individual confirms their understanding of these details, such as through signed declarations, website form acceptance of details or in person through questioning.

4.3.4 Collection from third parties

Where Healthguard collects personal information from another organisation, including our co-providers with whom we have a Third Party Arrangement, we will confirm that relevant notice has been provided to the individual, and if this has not occurred, we will undertake this notice to ensure the individual is fully informed of the information collection.

4.3.5 Using or disclosing personal information

Healthguard only uses or discloses personal information it holds about an individual for the particular primary purposes for which the information was collected, or secondary purposes in cases where:

- an individual consented to a secondary use or disclosure
- an individual would reasonably expect the secondary use or disclosure, and that is directly related to the primary purpose of collection
- using or disclosing the information is required or authorised by law.

4.3.6 Requirement to make a written note of use or disclosure for this secondary purpose

If Healthguard uses or discloses personal information in accordance with an 'enforcement related activity' we will make a written note of the use or disclosure, including the following details:

- the date of the use or disclosure
- details of the personal information that was used or disclosed
- the enforcement body conducting the enforcement related activity
- if the organisation used the information, how the information was used by the organisation
- the basis for our reasonable belief that we were required to disclose the information.

4.3.7 Cross-border disclosure of personal information

We do not proactively share information overseas, however it is disclosed that the Healthguard uses a student management system, incorporating cloud storage, which includes storage facilities outside of Australia. Healthguard takes reasonable steps to ensure that the recipient does not breach any privacy matters in relation to that information.

4.3.8 Use of personal information for direct marketing

Healthguard does not use or disclose the personal information that it holds about an individual for the purpose of direct marketing, unless:

- the personal information has been collected directly from an individual, and the individual would reasonably expect their personal information to be used for the purpose of direct marketing. E.g. reminders to previous learners to re-enrol for refresher training or other relevant courses, and
- we provide a simple method for the individual to request not to receive direct marketing communications (also known as 'opting out').

4.3.9 Adoption, use or disclosure of government related identifiers

Healthguard does not adopt, use or disclose a government related identifier related to an individual except:

- in situations required by Australian law or other legal requirements
- where reasonably necessary to verify the identity of the individual
- where reasonably necessary to fulfil obligations to an agency or a State or Territory authority
- as prescribed by regulations.

4.3.10 Quality of personal information

Healthguard takes reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete. We also take reasonable steps to ensure that the personal information we use or disclose is accurate, up-to-date, complete and relevant. This is important both when we initially collect the personal information, and then subsequent use or disclosure of the personal information.

Quality measures to support this include:

- internal training, practices, procedures and systems to audit, monitor, identify and correct poor quality personal information
- processes that ensure personal information is collected and recorded in a consistent format, from a primary information source when possible
- ensuring updated or new personal information is promptly added to relevant existing records
- providing individuals with a simple means to review and update their information on an on-going basis through our online portal
- reminding individuals to update their personal information at critical service delivery points
- contacting individuals to verify the quality of personal information where appropriate when it is about to used or disclosed, particularly if there has been a lengthy period since collection
- checking that a third party, from whom personal information is collected, has implemented appropriate data quality practices, procedures and systems.

4.4 ENSURING SECURITY AND ACCURACY OF PERSONAL INFORMATION

Healthguard takes active measures to ensure we are correct to retain personal information we hold, and also to ensure the security of personal information we hold. This includes reasonable steps to protect the information from misuse, interference and loss, unauthorised access, modification or disclosure.

We destroy or de-identify personal information held once the information is no longer needed for any purpose for which the information may be legally used or disclosed.

Staff are provided with training regarding privacy and records management as part of their induction with Healthguard. Information about updates to privacy requirements and reminders about requirements are provided to staff as needed.

5. PROCEDURES

5.1 Gaining access to personal information

1. Before giving access to personal information, Healthguard will confirm the identity of the individual making the request, to ensure it is the individual or a person who is authorised to make a request on their behalf.

   The minimum amount of personal information needed to establish an individual's identity is sought, which is generally an individual's name, date of birth, last known address and signature. When meeting the requesting party in person, identification may be sighted. If confirming details over a telephone conversation, questions regarding the individual's name, date of birth, last known address or service details may be confirmed before information is provided.

2. Healthguard will then confirm what information is required to be accessed and the format in which the information sought is required. Where the requested format is not practical, Healthguard will consult with the requester to ensure a format is provided that meets the requester's needs.

3. The next step is for Healthguard to respond to the request for access to information. The decision will be to complete the request or refuse the request:

Completion of request	**Refusal of request**
Healthguard will search records that we possess or control to assess whether the requested personal information is contained in those records. Any personal information found is to be collated ready for access. The access to the information is to be provided in the format in which it was requested. A request needs to be completed within 14 calendar days. The access to the requested information is to be provided free of charge.	A request may be refused if: • If the identity or authorisation access cannot be confirmed • There is another valid reason why Healthguard is unable to provide the personal information Refusal to provide access to records will be provided to the requester in writing. The notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual. The notifications is to be provided within 14 calendar days of receipt of the original request. There is to be no charge for this.

5.2 Correcting or updating personal information

1. Before correcting or updating personal information, Healthguard will identify the individual concerned and confirm their identity of the individual or party to whom the record relates.
2. Healthguard will then search the records that we possess or control to confirm if the pertinent personal information is contained in those records and assess the information to determine whether the requested update should proceed. This may include checking information against other records held by us or within government databases, in order to complete an assessment of the correct version of the information to be used.
3. Healthguard will then decide to correct/update the information as per the request or decline this update request:

Completion of request	**Refusal of request**
The identified personal information contained in the records is to be corrected or updated. The update will be notified to any relevant third parties of corrections made to personal information, if this information was previously provided to these parties. The update is to be completed within 14 calendar days. The update is to be provided free of charge.	A request may be refused if: • If the identity or authorisation access cannot be confirmed • There is another valid reason why Healthguard is unable or unwilling to update the personal information Refusal to update the information will be provided to the requester in writing. The notification will include reason(s) for the refusal, and the complaint mechanisms available to the individual. The notifications is to be provided within 14 calendar days of receipt of the original request. There is to be no charge for this. If requested by the individual, reasonable steps will be taken by Healthguard to associate a statement with the personal information that the individual believes it to be inaccurate, out-of-date, incomplete, irrelevant or misleading.

5.3 Making a privacy complaint

If an individual feels that Healthguard has breached its obligations in the handling, use or disclosure of their personal information, they may raise a complaint. We encourage individuals to discuss the situation with the Healthguard Operations Manager in the first instance, before making a formal complaint.

The complaints handling process is as follows:

1. The individual should make the complaint including details about the issue in writing to:

   Healthguard CEO
   c/o info@healthg.com.au
   Phone: 1300 001 302

2. Healthguard will investigate the circumstances included in the complaint and respond to the individual as soon as possible (within 30 calendar days) regarding its findings and actions following this investigation.
3. If after considering this response the individual is still not satisfied they make escalate their complaint directly to the Information Commissioner for investigation:

   Office of the Australian Information Commissioner
   www.oaic.gov.au
   Phone: 1300 363 992

6. RESPONSIBILITIES

Ensuring compliance with the Privacy Policy is the responsibility of all Healthguard staff and co-providers with whom Healthguard has a Third Party Agreement.

The Healthguard CEO retains accountability for the compliance of Healthguard with legislative requirements.

It is the responsibility of students and other third parties such as employers to provide accurate and up to date personal information to Healthguard in line with this Privacy Policy.

7. MONITORING AND EVALUATION

The Compliance Officer will monitor changes to Privacy Legislation requirements and recommend updates to the policy as required.

The policy is to be reviewed annually to ensure currency with requirements, and to be updated as changes to relevant legislation or Healthguard procedures occur.

The policy must also be reviewed and evaluated following any complaints relating to privacy.

8. DOCUMENTATION

Document control	
Version and Creation Date	Version 2.0 December 2020
File Location	RTO Compliance>Meeting Standards>Policy and Procedures
Review Due Date	• December 2021 – to ensure currency – with any redesign as required • As updates occur to relevant legislation
Creation Contact	Kathryn Burke - Compliance Officer
Final Approval	Cheryl Connolly - Owner/Acting CEO