Privacy Policy

This document sets out the policy of Defence Health Limited (ABN 80 008 629 481) and our subsidiaries (**Defence Health, we, us**) relating to the privacy of personal information (**Privacy Policy**). It applies to any individuals (**you**) whose personal information we hold.

1. How this Privacy Policy operates

Defence Health is committed to protecting the privacy of the personal information we hold. We are bound by the Australian Privacy Principles contained in the *Privacy Act 1988* (Cth).

You accept this Privacy Policy and expressly consent to the collection, use and disclosure of your and others' personal information as described in this Privacy Policy, when you use our website (www.defencehealth.com.au), our mobile applications, our products and services or enter into any communications with us.

In administering the policies, insurances and services we provide to our customers **(members),** we collect personal information not only about the member but also about other individuals covered by the policy such as a member's **dependants**, and people for whom the member is an **authorised representative**. Where the context requires, a reference in this Privacy Policy to a "member" includes dependants, people for whom the member is an authorised representative and people who have an authorised representative who acts on their behalf.

We may, from time to time, review and update this Privacy Policy to take account of new laws and changes to our operations. The updated Privacy Policy will also apply to information previously collected.

2. The kinds of personal information we collect

We only collect **personal information** (as defined in the Privacy Act, being information about an identified or reasonably identifiable individual) where we consider it to be reasonably necessary for our business functions or activities. The kinds of personal information we collect may include:

- your name, date of birth, age, gender, occupation, income-band and employment details
- the relationships, arrangements and correspondence between a member and the other persons involved in the policy or membership, who might include an authorised representative, health and other service provider, personal carer, attorney, spouse, partner, dependant or next of kin
- your postal address, email address, telephone number and social media handle;
- information about your membership status, products and services you buy from us, contribution history, premiums, claims, benefit payments and other transactions and interactions with us, including recordings of telephone calls
- information about any treatments, health services and other services provided to a member
- information relevant to the type of insurance you are purchasing, applying for or using. For example, for health insurance, this means information about your health, your relationship status, your eligibility to join, your Australian Defence Force status including your service category, details of any pre-existing conditions (how they occurred, treatment provider, details of hospital admission and period, legal representative, insurance company), DVA accepted conditions covered, history of health insurance cover (including level of cover, time held, age of entry to hospital cover, total absent days, previous fund, previous policy number, aged-based discount and claims history), reasons for any requested suspension of

insurance, your dealings with other health providers and insurance businesses, medical and general physical condition, and lifestyle

- where financial product advice is provided, sufficient personal information to assist you in completing an application form for the relevant insurance policy, and for us to manage the relevant insurance policy
- where an insurance policy is to be purchased as part of your superannuation, your tax file number
- your IP address, log-in details and website usage (see the Cookies section below)
- Medicare number, debit card, credit card, account and other banking details
- if you are an employee or prospective employee, we will collect all employment related information, including information from referees, police check, bankruptcy or Australian Securities and Investments Commission check, emergency contact and resume to be able to employ you and maintain your employment with us
- if you are an individual health service provider - your contact details, provider registration details, Government related details such as your Medicare provider number, details of the services you have rendered and charged for and claims made, bank account details, feedback about your services from our members; and aggregated claims data from the Australian Health Services Alliance Ltd and other sources.

3. How we collect your personal information

We will obtain your personal information only by lawful and fair means, and where practical, directly from you.

As a member, by using our services and providing personal information to Defence Health, you affirm that you consent, and you have the consent of any other individuals whose information you are providing, to Defence Health dealing with it under this Privacy Policy.

The circumstances in which we directly collect personal information will vary depending on the nature of the interaction. Some common ways we collect personal information directly from you are:

- when you provide information in the course of membership or health service provider dealings with us
- when you visit our office or attend a meeting or conference with us
- when we correspond with you by email, telephone, face to face or through our website or webchat
- when you apply for a position with us
- when you provide details on a form (including a webform or mobile application), such as application forms, claims form, as part of a dispute or complaint process, or when entering into a contract with us
- when you participate in a promotion, competition, promotional activity, survey, market research, subscribe to our mailing list or interact or follow our social media pages
- as you navigate our website, our social media pages (such as Facebook and Instagram) or use a mobile application to interact with us
- in the course of trade shows, promotions, displays, site visits or like events.

We may also collect your personal information from third parties and public sources including:

- when your employer or another service provider or entity you deal with provides personal information to us in the course of our relationship with them. Examples are where you as a health practitioner refer a member to another health practitioner we deal with; or where you as a member have instructed your employer to deduct premiums under a payroll deduction scheme
- health service providers who provide you, as a member, with services
- with your consent, from a previous health insurer about your previous or current cover with them
- from a recruiter or referral entity, where you are a prospective employee
- your legal representatives, authorised representatives and professional advisers
- service providers, brokers, agents, associates and related companies
- credit reporting agencies, referees, guarantors
- social media pages, marketing advisers, data aggregators and analytics service providers
- phone directories, web pages, membership lists, trade publications and directories, online search engines, professional and trade associations, ASIC, bankruptcy or court registry searches.

4. Using your personal information

We collect your personal information so that we can use it for our reasonable business purposes and provide products and services to our members.

Some further examples of how we use your personal information include:

- providing you with information about our services, offers, proposals or quotes
- processing applications, claims that you submit to us
- considering you for an employee position or service provider role
- administering and responding to your enquiry or feedback about our services
- conducting, and allowing you to participate in, a promotion, competition, promotional activity, survey or market research
- promoting and marketing current and future services to you, informing you of upcoming events and special promotions and offers
- analysing our products and services so as to improve and develop new products and services
- compiling data about your use of our products, website, mobile applications and social media pages so that we can design and target our marketing and promotions to other current and prospective customers
- compilation and maintenance of contact lists for use by us and our service providers
- facilitating our internal business operations, including fulfilment of any reporting, governance, account management, financial, legal and regulatory requirements
- research, publications, training, forums and reporting in relation to health, insurance, and other sectors in which we operate
- managing and improving the operation or navigation of our websites
- where necessary to comply with our legal obligations and enforce our legal rights

- other purposes for which you have provided consent.

5. Disclosing your personal information

We engage with a range of third parties in order to operate our business and provide services. We may disclose personal information to third parties for the same purposes as are set out in paragraph 4 above. Organisations to which we may disclose your personal information include:

- as required by law or regulatory bodies or in the interests of public safety, government bodies such as Medicare, the Australian Taxation Office, the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, the Australian Competition and Consumer Commission, the Australian Health Practitioner Regulation Agency, the Office of the Australian Information Commissioner, the Australian Cyber Security Centre the police or courts
- an enforcement body if we believe providing your personal information is reasonably necessary to assist the body in performing its function
- if we suspect that an unlawful activity or misconduct of a serious nature has been, is being, or may be engaged in (such as fraudulent claims or misconduct or overcharging by a member or health service provider) that relates to Defence Health and the personal information is a necessary part of our internal investigation or reporting of the matter to relevant authorities
- industry, professional or government organisations
- service providers we use to operate our business such as:
  - information technology, social media and platform providers
  - finance, insurance, underwriting, and re-insurance businesses
  - marketing and communications agencies
  - mailing houses, freight and courier services
  - printers & distributors of marketing material
  - advisers such as accountants, marketers, data and business analysts, recruiters, debt collectors, auditors & lawyers and in each case, their representatives, contractors, agents and distributors.

When making public or disclosing information that was prepared using personal information, where practical we will de-identify, aggregate or anonymise the information to remove the personal information.

For the purposes of this Privacy Policy and unless circumstances suggest otherwise, a person aged 16 years and above will be considered capable of making their own privacy decisions and managing their own information and claims on the policy. Defence Health will take instructions from the person who is authorised to make relevant decisions relating to health insurance and health matters generally for that person or dependant.

Unless otherwise instructed by an insured person aged 16 years or above, we may also provide personal information about a member to any other person amongst that group. Upon request, by any member or dependant 16 years or over, we will make reasonable efforts to keep their personal information private from other members on the policy, in particular where health and other sensitive information is concerned, but this may be subject to limited exceptions.

6. Do you have to provide personal information?

You can refuse to provide personal information. A refusal may mean that we are unable to provide the service you, a member or an organisation has asked for. For example if we propose to apply a service or process a claim we may be unable to do so.

7. Cookies and website use

We may collect personal information about you when you engage with us online via our website(s), email, and social media accounts; when you like our posts on social media, leave any information via a post, comment or review or request to be involved in one of our campaigns or competitions or use any of our services or otherwise enter information into any comment fields, events and other community forums sponsored by or affiliated with Defence Health.

We do this by using cookies and third-party analytics and advertising services. We use this information to improve our website, assist us in our advertising and marketing campaigns including marketing to other current and prospective customers, to provide you with information on our products and services that we think is most relevant to you and to enable us to measure the progress of our marketing activities.

"Cookies" are data files (of letters and numbers) that we store within the hard drive of your computer when you interact with our website. When you visit our website, our servers collect routine logging information such as the pages visited, the time of your visit, your web browser and device type, geo-location and the IP address associated with your request. We also collect referring URLs of website you have visited or will visit, data about the activities you undertake and how you interact with us online, such as what data is displayed, clicked on or shared, and the length of time you spend on our site or page.

Typically, the information we collect in connection with your online activities is anonymous, aggregated, de-identified, or otherwise does not reveal your identity.

If you visit third party website or social media platforms via a link from our website or pages, they may also collect your personal and other information about you. Their collection and use of your information are subject to the terms and conditions and privacy policy that apply to their services as disclosed by them. Defence Health is not responsible for their handling of your personal or other information.

Please note that many online forums, including our social media pages, are public and others can see what information you disclose. You are not required to submit any information or participate. We may, but are not required to, monitor any activity and remove content within our control or block participants. Any information you post or disclose in this way is public and we cannot control its use.

8. Direct Marketing

If we hold your personal information, we may use or disclose that information for direct marketing if:

- we collected the information from you or another source in accordance with this Privacy Policy
- it is reasonable for us to use or disclose the information for that purpose
- we provided you with a way to opt out of receiving direct marketing from us
- you have not made such an opt out request.

Whenever we send you marketing material, we will always inform you how you can opt out of our mailing list. We will implement your request free of charge within a reasonable timeframe.

9. Protecting your personal information

We store information in different ways, including paper and electronic form. We take reasonable steps to protect it from misuse, interference, loss, unauthorised access, human error, modification or disclosure including:

- secure password protected databases for storage

- limited access to personal information on a need to know basis within Defence Health
- confidentiality requirements of Defence Health employees and contractors
- training of staff
- security for access to our systems including firewalls and encryption
- document storage security requirements
- access controls for our building
- limiting the provision of personal information to third parties on a need to know basis, and subject to commitments from them that are similar to the commitments we make in this Privacy Policy
- regular testing of our information security controls to ensure they are appropriate.

We also take reasonable steps to check that the service providers, health providers and third parties we disclose information to have good security processes in place.

Due to the nature of electronic communications and the public internet, we cannot guarantee that personal information will be protected against unauthorised access or misuse, and we do not accept any liability for breaches due to human error, malicious or inadvertent disclosure, technology flaws or misfunction, or the improper actions of unauthorised third parties.

We will retain your personal information for as long as necessary to fulfil our obligations to you, to protect our legal interests, to comply with regulation, or to manage our business appropriately. Once those reasons for retaining your personal information no longer apply, we will take reasonable steps to destroy your personal information or to ensure that your personal information is de-identified.

10. Accessing and disclosing your personal information overseas

While we prefer to store data including personal information on local Australian servers, in some cases we may disclose your personal information to third party platform and service providers operating outside Australia. Additionally in some instances Defence Health may have employees and contractors who reside overseas and have access to your personal information. Overseas regions to which we currently send information are:

- Ireland
- Other parts of western Europe
- USA
- New Zealand
- India

We may also store your personal information on servers based overseas or in the "cloud" or other types of networked or electronic storage, which may be distributed in multiple jurisdictions. Where "cloud" computing is used by us, your personal information may be viewed from overseas jurisdictions to repair system faults, and as far as is reasonable, we have contractual protections for your personal information in these scenarios.

11. Accessing and correcting your personal information

You may request access to and/or correction of any of our records containing your personal information. To request access and/or correction please contact us on 1800 335 425 or via email to info@defencehealth.com.au. We will respond to your request within a reasonable period of time. On the basis that it is reasonable and practicable to do so, we will give you access to the information requested and/or correct the relevant information.

If we refuse your request, we will provide a written notice setting out the reasons for the refusal and how you can complain about the refusal.

12. Resolving your privacy issues

If you have any issues you wish to discuss with us or if you're concerned about how we have collected or managed your personal information, please contact our Privacy Officer using the the details below.

For information about privacy or if your concerns are not resolved to your satisfaction, you may contact the Office of the Australian Information Commissioner at www.oaic.gov.au and on 1300 363 992.

13. How to access this Privacy Policy

This Privacy Policy is available on our website. A printed copy of the Privacy Policy can be obtained free of charge by contacting us directly.

Our Privacy Officer can be contacted at:

Attn: Privacy Officer
Defence Health
Level 7, 380 St Kilda Road
Melbourne VIC 3004
Phone: **1800 335 425**

Email:legal@defencehealth.com.au

Last Updated: December 2023