HAMBS

Policy

Privacy

1. Introduction

This policy outlines how HAMBS manages *information*[1] in accordance with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth).

The information in this document is intended for those individuals whose personal information we may collect while carrying out our business functions and providing services to our customers. However, it does not apply to employee records we maintain in relation to our employees.

2. Our business functions and activities

We collect, hold, use and disclose personal information to carry out our business functions and provide services in accordance with our agreements with our customers. Those business functions and customer services include:

- Providing consulting with private health insurance industry (PHI) stakeholders and providing PHI advice and advocacy
- Providing managed hosting services
- Developing software and other technical solutions
- Providing application and technical support
- Providing PHI related training
- Providing integration services to support our customers' business processes and operations
- Providing facilities for processing of e-commerce transactions, including HICAPS, HealthPoint and ECLIPSE
- Providing eligibility checking facilities for hospital providers
- Providing claims fraud protection and detection services
- Managing customer, supplier, business partner and other stakeholder relations
- Communicating with the public and stakeholders through our website and social media
- Assessing suitable candidates for career opportunities within HAMBS

We define our and our customers' obligations for customer data in our agreements with our customers. Customers retain full ownership of their data when using our services and remain responsible for the personal information that they collect, hold, use and disclose.

If you hold health insurance with, or receive other services from, one of our customers or their service providers, you should refer to their privacy policy in addition to this privacy policy. You should direct any privacy-related questions about those organisations' products or services directly to them.

3. Collection and use of personal information

We collect personal information about individuals which is reasonably necessary to carry out our business functions and provide service to our customers. The types of personal information which we collect and hold about you may vary depending on the nature of our interactions with you.

[1] Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Health fund members and health service users

As a hosting provider and integrator most of the data we hold is collected by and transferred to us by our customers and their agents, brokers and service providers. We define our and our customers obligations for customer data in our agreements with our customers.

We collect, hold and process this data on the basis that our customers to which we have contracted our services and their agents, brokers and service providers have made appropriate privacy-related disclosures to you and obtained your consent to the disclosure of your personal information to, and its collection by, HAMBS.

If you are a customer of one of our customers or their agents, brokers or service providers the information they may collect about you and may disclose to us include

- name and contact details (including address, email and phone numbers)
- age or date of birth
- gender
- government related identifiers such as your Medicare number[2]
- financial information such as your bank details
- information about your preferences relevant to any marketing activities
- sensitive information such as details about your health and health services provided to you and other claims related information
- other information related to transactions and dealings between you and your health fund and your health service providers

We only use this information to provide services to our customers and their service providers in accordance with the terms and conditions of agreements with our customers. For example, to

- provide the software and technical solutions that process private health insurance policies, premiums, claims and benefit payments.
- provide software and technical solutions to enable integration and e-commerce transactions between our customers' and other service providers such as hospitals, doctors, allied health providers, Services Australia, HICAPS, HealthPoint and financial institutions.
- provide claims fraud protection and detection services.
- provide application and technical support.

For further details you should refer to the privacy policies of your health insurer and your health service providers in addition to this privacy policy.

HAMBS customers, suppliers, and business partners

We may collect contact details and some other personal information about you if you are an employee of one of our customers, suppliers or business partners.

The information we may collect about you include

- name and contact details (including business address, email and phone numbers)
- title or role or position that you hold within your organisation
- information related to courses and other training you undertake with us
- information that you as a customer provide to us in relation to service desk tickets, requests, customer engagement and other interactions with us
- information that you as a supplier or business partner provide as part of providing your service

[2] Although the nature of our services require us to collect, store, use and disclose certain identifiers created or issued by the Commonwealth Government (such as Medicare numbers), our systems are configured so that these identifiers are not used as a means of identifying the individual.

We may use this information to

- Manage our ongoing relationship with you and your employer.
- Provide you with our products and services or receive products and services from you or your employer.

Prospective employees and applicants

We collect personal information when recruiting people to work with us, such as name, contact details, qualifications, and work and study history (including references and other information included in a resume or cover letter as part of the application process).

We may use automated tools to assist in evaluating applications.

- For example, you need to meet certain pre-screening criteria (such as Australian working rights) in order for your application to progress.
- Additionally, to set prospective employees up for success, online skill testing platforms may be used to determine candidate technical proficiency. Applicants who do not achieve required results may not proceed further in the recruitment process.

We determine our personal information retention periods based on our business needs and applicable legal obligations. Information is retained only as long as necessary to fulfill the original purpose of collection, as well as any other legitimate, related purposes that are permitted.

Before offering you a position, we may collect additional details such as your tax file number and superannuation information and other information necessary to conduct background checks to determine your suitability for certain positions.

Websites

We may collect personal information about you when you use our websites (including when you use our website and what you do, and the information you input, while using it).

We collect information such as IP addresses and domain names via the use of website cookies if the privacy settings you have chosen on your device allow it to accept our cookies. Cookies do not identify an individual personally but may link to a stored record about them. These cookies allow us to retain a personal record so that we can provide our service to you more effectively. You can, if you wish, access the content on our website without accepting cookies, but will find navigation and returning to our website easier if you accept cookies.

We use this information for analytics purposes. We will not attempt to identify you or your browsing activities from clickstream data collected by our webserver except in the circumstances specified below.

If we or any authority suspect that unauthorised access or use of the website has occurred or may occur or be attempted, we may gather, use and disclose more extensive information than indicated above regarding access or attempted access to the website for the purposes of prevention, detection, investigation or prosecution.

Our website may contain links to other websites. HAMBS is not responsible for the privacy practices of these other websites.

Social Media

We use social networking services such as X (previously Twitter), Facebook, Instagram and LinkedIn to communicate with the public about our work. When you communicate with us using these services, we may collect your personal information, but we only use it to help us to communicate with you and the public. The social networking service will also handle your personal information for its own purposes. These services have their own privacy policies.

Direct marketing

HAMBS does not provide direct marketing communications to individuals.

Anonymity

Where possible, we will allow you to interact with us anonymously or using a pseudonym. However, in most of our functions and services it is not practicable for you to remain anonymous or use a pseudonym. If you do not wish to provide any required personal information, then you should not proceed with the completion of the relevant process.

Use of Automated decision-making (ADM) and customer obligations

Some HAMBS services and technical solutions support or enable our customers to use automated decision-making technologies for processing personal information. For example, our software solutions assist customers in automating aspects of claim assessment, fraud detection, and eligibility checks.

Where this occurs, our customers remain responsible for ensuring they meet their legal obligations in relation to automated decision-making, including:

- Making appropriate privacy disclosures to individuals,
- Ensuring the use of ADM is fair, lawful, and transparent,
- Providing individuals with meaningful information about the logic involved and the consequences of automated decisions, where required,
- Offering avenues for review of significant decisions made solely by automated means, where applicable.

Other than what we have disclosed under *Prospective employees and applicants* above HAMBS does not independently make decisions about individuals using automated tools. We provide the technical solutions, support, and secure hosting infrastructure necessary for our customers to configure and operate these processes. We work with our customers to ensure our services are designed and operated in a way that supports their compliance with applicable privacy and regulatory obligations.

4. Disclosure of personal information

In using and storing your personal information, we may pass on your personal information to third parties when:

- Required as part of providing services in accordance with the terms and conditions of agreements with our customers to which we have contracted our services. For example,
    - when providing integration between our customers different software systems such as integrating data into a customer relationship management (CRM) system,
    - when providing verification of membership and eligibility to a hospital or other health service provider in relation to a treatment,
    - when transferring memberships between health funds,
    - when sending claim data to Services Australia for the payment of Medicare benefits, or
    - when paying claims via a facility such as HICAPS.
- Another organisation or person provides a service for, or to, us and has an agreement with us that includes confidentiality provisions. For example, data centre providers, software suppliers and IT and business service providers.
- Required or authorised by law. For example, we may provide information to regulatory bodies, such as APRA, or government enforcement agencies.

Disclosure to overseas recipients

Our managed hosting services use data centres located in Australia. We do not currently transfer personal information to overseas recipients. However, there may be occasions where we are required to do so in order to provide our services or manage our relationship with you. If we transfer your personal information outside Australia, we will only do so where:

- we are authorised or required by law to disclose to the overseas recipient; or
- the overseas recipient is subject to laws or a binding scheme substantially similar to the Australian privacy principles; or
- you have provided informed consent.

5. Security of personal information

HAMBS is committed to protecting the personal information we hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. We maintain a comprehensive information security program designed to safeguard data throughout its lifecycle. This includes physical, administrative and technical controls aligned with industry standards and our contractual obligations.

We apply layered security controls across our environments, including secure managed hosting, encryption, access controls, network segmentation, vulnerability management, and continuous monitoring. Access to our systems and to customer data is restricted to authorised personnel on a need-to-know basis, and all staff are bound by confidentiality obligations and regularly trained on information security and privacy practices.

HAMBS operates under a shared responsibility model. Our customers remain responsible for ensuring that their collection, use and disclosure of personal information complies with privacy laws, including where they use our systems or services to support automated decision-making.

We maintain a comprehensive incident response framework, including processes to support timely containment, assessment and notification of any suspected or actual data breaches.

We regularly review and update our security practices and undertake independent assessments to verify their effectiveness. We also take reasonable steps to ensure that the personal information we collect, use and disclose is accurate, complete and up to date.

Shared responsibility for privacy

As a service provider, HAMBS operates under a shared responsibility model. While HAMBS is responsible for securing the systems and platforms we operate, our customers are responsible for how they collect, input and use personal information within those systems. Customers must ensure their own privacy notices, consent mechanisms, and data governance practices comply with applicable privacy laws.

6. Accessing and correcting your personal information

Under the Privacy Act (Australian Privacy Principles 12 and 13) you have the right to ask for access to personal information that we hold about you and ask that we correct that personal information.

Where your access or correction request relates to your private health insurance policy or related services you should contact your private health insurer directly to access or correct the information as they are best placed to assist you as the primary data holder. We may pass on your access or correction request to your health insurer if it relates to data that they control. We will advise you if we have passed on your request.

You can ask for access to or correction of personal information that we hold by contacting us in writing using the contact details below.

If you ask, we will give you access to your personal information, and take reasonable steps to correct it if we consider it is incorrect, unless there is a law that allows or requires us not to. If we refuse to give you access to, or correct, your personal information, we will notify you in writing setting out the reasons.

If we make a correction and we have disclosed the incorrect information to others, you can ask us to tell them about the correction. We will do so unless there is a valid reason not to.

If we refuse to correct your personal information, you can ask us to associate with it a statement that you believe the information is incorrect and why.

We will ask you to verify your identity before we give you access to your information or correct it.

We will respond to your request within 30 days.

We may charge a fee for processing your information access request.

7. How to make a complaint

If you wish to complain to us about how we have handled your personal information you should complain in writing.

If we receive a complaint from you about how we have handled your personal information we will determine what (if any) action, we should take to resolve the complaint.

We will tell you promptly that we have received your complaint and then respond to the complaint within 30 days.

8. How to contact us

Address	The Privacy Officer c/o Risk and Compliance Manager HAMBS Level 4, 169 Pirie Street ADELAIDE SA 5000
Email	admin@hambs.com.au

9. Definitions

Term	Definition
HAMBS, *we*, *us* or *our*	HAMB Systems Limited (ABN 44 053 315 772)
Personal information	*Personal information* is any information or an opinion about an identified individual or an individual who is reasonably identifiable and includes health information and other sensitive personal information (as defined in the Privacy Laws)
Privacy laws	*Privacy Laws* means the then applicable laws and regulations governing our collection use and disclosure of personal information and includes the Australian Privacy Principles
Site	*Site* means any website or online service provided by us or on our behalf
You	"you" refers to the individual who is the subject of personal information submitted to us or any person submitting personal information relating to others to us