

# Privacy Policy

## Policy Statement

This policy applies to the TUH brand of Teachers Federation Health Limited (Teachers Health).

TUH is committed to protecting any personal information entrusted to or obtained by us.

## We will achieve our commitment by:

- Following processes for how we collect, use, store and disclose personal information that comply with this policy; and
- Complying with the Privacy Act 1988, including the Australian Privacy Principles.

The Privacy Act takes priority if there is any discrepancy between it and this policy.

## Policy Details

### What is personal information?

Personal information is any information or opinion about you that could reasonably be expected to identify you, regardless of whether the information or opinion is true, or whether it is recorded in a hard or electronic or any other material form.

Sensitive information is a subset of personal information which is subject to greater controls. It includes health information and union membership details. For the purposes of this policy, any reference to personal information includes sensitive information.

### Why do we collect and use personal information?

We collect personal information primarily to enable us to provide private health insurance benefits and health care services and programs.

For example, your personal information could be collected and used to:

- Manage your membership and our relationship with you;
- Approve claims for hospital, medical and other health services;
- Verify eligibility for benefit payments;
- Provide products and services that you have requested;
- Make services provided by contracted third parties available to you;
- Record details of any treatment you may receive;
- Update your payment details;
- Respond to your enquiries;
- Meet internal functions such as administration, learning and development, accounting, auditing, risk management and fraud protection;
- Conduct research and analysis for product development, service improvement and marketing purposes;

- Evaluate existing, and/or develop new products, benefits, services and processes;
- Inform you of products, benefits or services;
- Investigate and resolve disputes and/or complaints;
- Supply you with advertising that is more relevant to you, when you have visited our website or other websites that promote our products, or have otherwise expressed an interest in our business (for example to remind you of products and services you were interested in, or to tell you about special offers and discounts); and
- Comply with our legal obligations, which include providing some personal information to government agencies.

We have agreements with itsmygroup, FujiFilm, and the Australian Health Service Alliance (AHSA) to collect, use and disclose your personal information, including your health information (“your information”). We use the services of itsmygroup when you submit an online request for a quote or indicate your interest in our services. FujiFilm, assists with the distribution and processing of mail and claims. AHSA provides technical support in claims processing and data analytics. Your information may be used by these entities for the purposes of responding to your enquiries, finding the right level of cover for you, establishing a membership with us, providing health services to you, managing the funding of those services, or otherwise as required by law. In order to provide these services, itsmygroup, FujiFilm, and the AHSA may collect information from you, receive your personal information from us, use your information, and disclose your information to us or your health service provider.

itsmygroup privacy policy can be found at <https://itsmy.com.au/privacy/>.

AHSA’s privacy policy can be found at [www.ahsa.com.au/web/ahsa/privacy\\_policy](http://www.ahsa.com.au/web/ahsa/privacy_policy).

FujiFilm privacy policy can be found at <https://www.fujifilm.com/au/en/privacy>.

## **Employee details**

We also collect personal information from our employees. This information will be used to make contact with employees regarding operational matters and in the event of an emergency; to share relevant updates and notices; to provide wages and other benefits; and to comply with our legal obligations, which include providing some personal information to government agencies.

## **Direct marketing**

We will only use or disclose your personal information for direct marketing purposes about our own products and services, or those from other providers that you may reasonably expect us to communicate with you about. You may opt out of marketing communications at any time by letting us know or by amending the settings on your relevant digital platform.

## **Policy holder and membership**

The health insurance policy holder is the person in whose name the membership is held and holds the legal responsibility for the membership. We direct all correspondence to the policy holder unless we are responding to a request from another person covered by that policy, or a suitable alternative authority or direction is in place.

## What personal information do we collect?

The personal information we collect and hold depends on the nature of the relationship we have with you and the extent to which you have used our services or made claims. Information will only be collected with your consent (refer to 'How do I provide consent?' below) or as permitted by law.

The type of personal information we may collect about you may include:

- Identification details such as name, gender, marital status and date of birth;
- Contact details such as home, postal and email address and phone numbers;
- Legal details such as Power of Attorney or Guardianship Orders;
- Government details such as Medicare number, tax file number (Employees only) and Private Health Insurance Rebate registration;
- Financial details such as bank or other financial institution account and credit card details;
- Private health insurance details such as current and past levels of cover, changes of cover, cancellations and suspensions of membership;
- Sensitive information such as health and medical details including claims and services or programs that we have provided, or you have accessed through us, and union name and union member number;
- Recordings of calls and records of email correspondence between us; and
- Browsing history if you use our website or app.

## Providing consent

By making an enquiry about our products or services; becoming a member, patient or client; visiting our website, social media pages or mobile app; requesting an online quote; completing an online or physical form; contacting us by email or phone; making a claim for benefits; or otherwise making use of services offered by us (including where the services are provided by organisations contracted by us), you are regarded as having consented to the following:

- The collection of personal information by us, including from third parties; and
- The use and disclosure of personal information;

in accordance with this policy.

If the health insurance policy held by you includes anyone aged 16 and over, it is important that you obtain their approval to provide their personal information to us. If you provide such information, we will consider that you have obtained this consent. We will also assume that you have authority to provide us with the personal information of anyone covered by the policy who is aged under 16.

### **Can I withdraw consent?**

You are entitled to withdraw consent at any time by contacting our Customer Contact Centre or our Privacy Officer.

### **Can I deal with TUH anonymously?**

You can deal with us anonymously where it is lawful and practicable to do so. For example, for quotes, some general enquiries about membership and benefits we pay for a particular procedure, there will usually be no need for you to provide your personal details.

If you withdraw your consent to collect, use, store and disclose some or all of your personal information that we may need, or wish to deal with us anonymously, we may not be able to provide you with many of the benefits or services that we offer.

## How do we collect personal information?

Where it is reasonable and practicable to do so we will collect personal information directly from you, such as when you:

- Contact us or express your interest in our services by phone, email, online (including webchat and videoconferencing) or SMS, in writing or in person;
- Request an online quote;
- Respond to our direct marketing surveys or campaigns;
- Submit an application for one of our products;
- Submit a variation to the type or level of cover or persons covered;
- Lodge a claim;
- Use our website or an app we have established, including submitting an online form or health risk assessment questionnaire;
- Interact with our social media pages;
- Arrange and receive a health care service; or
- Participate in our health management programs.

### Website

Depending on how you use our website, we may collect your personal information indirectly through this channel using either first or third-party cookies.

Cookies are small pieces of data sent by your browser when you use many websites, including our website. The cookies are stored on your computer or device. They capture information, such as your viewing preferences, to make your use of the website more efficient.

We collect cookies data to help us understand which pages are viewed the most, when peak usage times occur, along with other information that helps us improve the content and make navigation easier for you.

You can choose to disable cookies through your browser settings, however please be aware that doing so may result in a less than optimal user experience.

We may also use Google Analytics and similar tools from other organisations such as YouTube to better understand how our website is used. This makes information stored in server logs available to these companies. The information is aggregated and does not identify individuals.

Third-party vendors, including Google, show our ads on sites across the internet. Third-party cookies from Google and other organisations analyse website visits and provide ads based on these visits using applications that include:

- Remarketing with Google Analytics,
- Google Display Network Impression Reporting,
- DoubleClick Platform integrations, and
- Google Analytics Demographics and Interest Reporting.

You can choose to disable Google ad personalisation by following [this link](#).

### **Facebook Pixel**

Our website uses a Facebook Pixel. This allows us to track browsing behaviour on our websites and measure the efficacy of Facebook advertising by reporting on the actions people take after viewing our ads.

We may use your personal information to create a customer list ('Custom Audience') that we can use to advertise to you, or to create a 'Lookalike Audience' to find new people who share similar behaviours and interests as you. To make a 'Custom Audience' for our use on Facebook, we would upload information about you which would include an 'identifier' (such as email, phone number, address) to Facebook via direct integration. Facebook would then create a Custom Audience or lookalike audience for us to use for marketing purposes. When we upload the customer list to Facebook for the matching process, the information is 'hashed' so that your personal information is unidentifiable at an individual level. Hashing is a type of cryptographic security method that turns your identifiers into randomised code.

If you have a Facebook account, you can manage your Facebook Privacy Settings by following [this link](#).

We may use Custom Audiences on other online platforms such as LinkedIn and Instagram.

### **Visual Website Optimizer**

The TUH website uses the Visual Website Optimizer web analysis service by Wingify Software Private Limited, Inc., which is used for multi-version tests. This service uses cookies to identify a user's browser and to analyse the use of this website. The cookies placed by Visual Website Optimizer do not collect personal data.

More information about how Visual Website Optimizer processes your data can be found at <https://vwo.com/privacy-policy/>. You can disable Visual Website Optimizer tracking at any time by following the instructions at <https://vwo.com/opt-out/>.

### **What about linked websites?**

On our website, we provide links to third party websites. Since we do not control these sites, we encourage you to review the privacy policies posted on these third-party sites. We are not responsible for any practices on linked websites that might breach your privacy.

### **Information collected from third parties**

We may collect information about you from another person or organisation. For example:

- Other individuals on your health insurance policy, e.g., a family membership;
- Your hospital or a health provider;
- Persons or organisations necessary to establish eligibility for benefits where services claimed may be paid, at least in part, from another source;
- A provider contracted by us to provide services on our behalf, including research and marketing. These services include collecting details of potential members;
- Financial institutions;
- Claiming software providers (such as HICAPS);

- Your employer, if you are part of a payroll deduction scheme;
- Another health insurer if you are transferring your membership; or
- Another person that you have provided authorisation to deal with us.

## How do we use Artificial Intelligence?

We are committed to leveraging artificial intelligence (AI) to enhance services, improve member experiences, and streamline operations while upholding ethical standards and complying with Australian laws.

Our AI tools are designed to reflect our commitment to ethical use, transparency, and member-focused outcomes. The AI tools used by TUH primarily leverage machine learning forms of AI. However, vendors are increasingly incorporating more advanced AI technologies over time. We carefully evaluate these new advancements, before deciding to adopt them.

Our AI principles ensure transparency in operations, accountability for AI-generated decisions, and full compliance with all applicable laws, regulations, and industry standards. Additionally, our Artificial Intelligence policy prohibits using Personally Identifiable Information and Health Information for employees or members within AI systems and establishes clear guidelines for the responsible use of TUH-approved AI solutions.

## When do we disclose personal information?

TUH utilises a range of electronic records retention tools. As with any internet-facing environment, it is not possible for us to guarantee absolute security and there is a possibility that unauthorised access may be gained by cyber criminals. TUH uses physical, electronic, and procedural safeguards to protect your personal information. We regularly review our cyber security position and aim to minimise this risk.

We will only actively disclose information to third parties (who are not members of your policy) when:

- You have authorised, or would reasonably expect us to provide information. For example, when providing verification of membership to a hospital or other health service provider before or after receiving treatment, when transferring between health funds, when sending claim data to Medicare for the payment of Medicare benefits, or 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, software suppliers, data processing and analysis, publishers, printers, mail houses, health providers, electronic claims facilitators, record management providers, financial institutions, marketing agencies and research bureaux;
- We obtain expert advice such as from medical referees, claims consultants and legal and other professional advisers;

- You receive a health care service or become eligible to participate in a health program provided by a third party on our behalf, for example, our wholly owned subsidiary TUH Health Care Services, or contracted chronic disease management program providers;
- You receive a health care service from one of the co-located Health Hub providers who provide dental, optometry, podiatry, massage, physiotherapy and audiology services - in which case, as an integrated health care centre, your personal and/or health information may be shared between health care providers as relevant to your clinical needs, and with administrative staff for billing and appointment bookings;
- We use or assist service providers, other health insurers or other third parties to help us prevent and detect fraud or inappropriate claiming;
- Required or as permitted by law. For example, we provide information to regulatory bodies, government enforcement agencies (including overseas), complaints adjudicators and others; or
- The safety of our members or if the safety of others in the community is at risk.

We may also disclose information to other individuals on your policy, or to any person that you have authorised to act on your behalf. To act on such an authority, we will need your written permission or a copy of a Power of Attorney, or similar document.

If you use our services at the Fortitude Valley Health Hub and you are also a TUH fund member then we may share your information across these services (excluding sensitive health information), for example a request to update your address details with our Health Fund will be shared with the Health Hub to ensure your personal information is accurate across all of our information management systems.

In the event of unauthorised access to, or disclosure of, your personal information, TUH has procedures in place to immediately take appropriate action consistent with our Privacy Act obligations.

### **When do we send personal information overseas?**

At times we may send your information to, or allow access by, organisations outside Australia that we have contracted with (directly or indirectly via an Australian organisation) to provide services on our behalf. We will only do this where we are satisfied that the recipient of the information will handle and protect your information in a manner that is consistent with the Australian Privacy Principles and this Privacy Policy and:

- We have your consent (refer to 'How do I provide consent?' above); or
- We have a contractual obligation to do so or there is some other identifiable benefit to you; or
- Where we are required to by law.

We may disclose personal information to organisations or persons in the following countries: Canada, India, Japan, New Zealand, Singapore, United Kingdom, South Africa, North America, Germany and United States.

## How do we store your personal information?

We take all reasonable steps to protect your personal information from unauthorised access, misuse or disclosure.

Your information is kept until it is no longer required for any purpose. Information that is no longer required will be securely destroyed or deidentified. In some circumstances, your information may be retained for a longer period, for example to comply with statutory or auditing requirements, or where destroying this information would negatively impact on another of our members. All personal information held by us is stored at our restricted-access premises, at secured off-site premises, or in secured electronic environments.

Policies and procedures are also in place to protect personal information from misuse, loss or unauthorised access, modification or disclosure. We will ensure the ongoing adequacy of these policies by reviewing these documents regularly and by conducting regular employee training.

## What do we do with unsolicited personal information?

If we come into possession of personal information that we did not request, we will destroy it as soon as practicable, and if lawful and reasonable to do so.

## Accessing and correcting your personal information

Any dependant aged 16 years and over may access their own personal information.

Any other adult member under a policy can access personal information, including financial, billing, benefit and health information about other members on the policy via our Member Services Online facility, the mobile App, or upon request.

You must discuss your options with us if you do not want to provide access to your personal information to other members of your policy.

### **Responding to an access request**

We will endeavour to meet all appropriate requests for access; however, access to some information may be denied, including where:

- We no longer hold the information;
- Denying access is required or authorised by or under law;
- Providing access would have an unreasonable impact upon the privacy of other individuals;
- Providing access would pose a serious threat to the life or health of any individual;
- The request is frivolous or vexatious; and
- Access relates to existing or anticipated legal proceedings or a court order.

Our Privacy Officer will advise the reasons why we cannot give members access to the information requested.

Under current privacy laws, we have up to 14 days to respond to a written request and 30 days to grant access.



### **Correcting your personal information**

We will take reasonable steps to ensure the personal information collected, used or disclosed is accurate, complete and up to date.

If you believe that your personal information is not accurate, please advise us. We will amend your records promptly unless we disagree with the change requested. If that occurs, we will explain the reason and document it on your records.

#### **Is there a cost?**

There is no charge for correcting your personal information or requesting access to it. However, you may be charged a processing fee for retrieving and providing the information depending on the complexity of the request. We will advise if a charge may apply when we respond to your request.

### **How do we communicate with you?**

Where you have provided us with an email address, including by using one of our Apps, we will use that as the main method of communicating with you, unless you have nominated another preferred method. We may also contact you by phone, mail, SMS or push notifications.

You can choose how we communicate with you by letting our Customer Contact Centre know.

### **Who do I contact if I want more information or to make a complaint?**

If you have a question on this Privacy Policy or would like further details of how we may collect, use, store and disclose your personal information please contact our Privacy Officer.

You should also contact our Privacy Officer if you have any concerns or a complaint about how we have handled your personal information or have complied with the Australian Privacy Principles. We will acknowledge receipt within three working days and aim to resolve any complaint as soon as possible.

#### **Office of Australian Information Commissioner (OAIC)**

Further information about the Privacy Act can be found at the website of the OAIC – [www.oaic.gov.au](http://www.oaic.gov.au). You can also contact the OAIC if you are not satisfied with our response or the way we have handled your complaint.

### **Contact Details**

#### **TUH**

PO Box 265/438 St Pauls Terrace  
Fortitude Valley QLD 4006  
Email: [privacyofficer@teachershealth.com.au](mailto:privacyofficer@teachershealth.com.au)  
Phone: 1300 363 992

#### **Office of Australian Information Commissioner**

GPO Box 5218  
Sydney NSW 2001  
Phone: 1300 363 992