



**THE SENATE  
SENATE FINANCE AND PUBLIC ADMINISTRATION  
REFERENCES COMMITTEE**

**Delivery of National Outcome 4 of the National Plan to Reduce Violence Against  
Women and Their Children.**

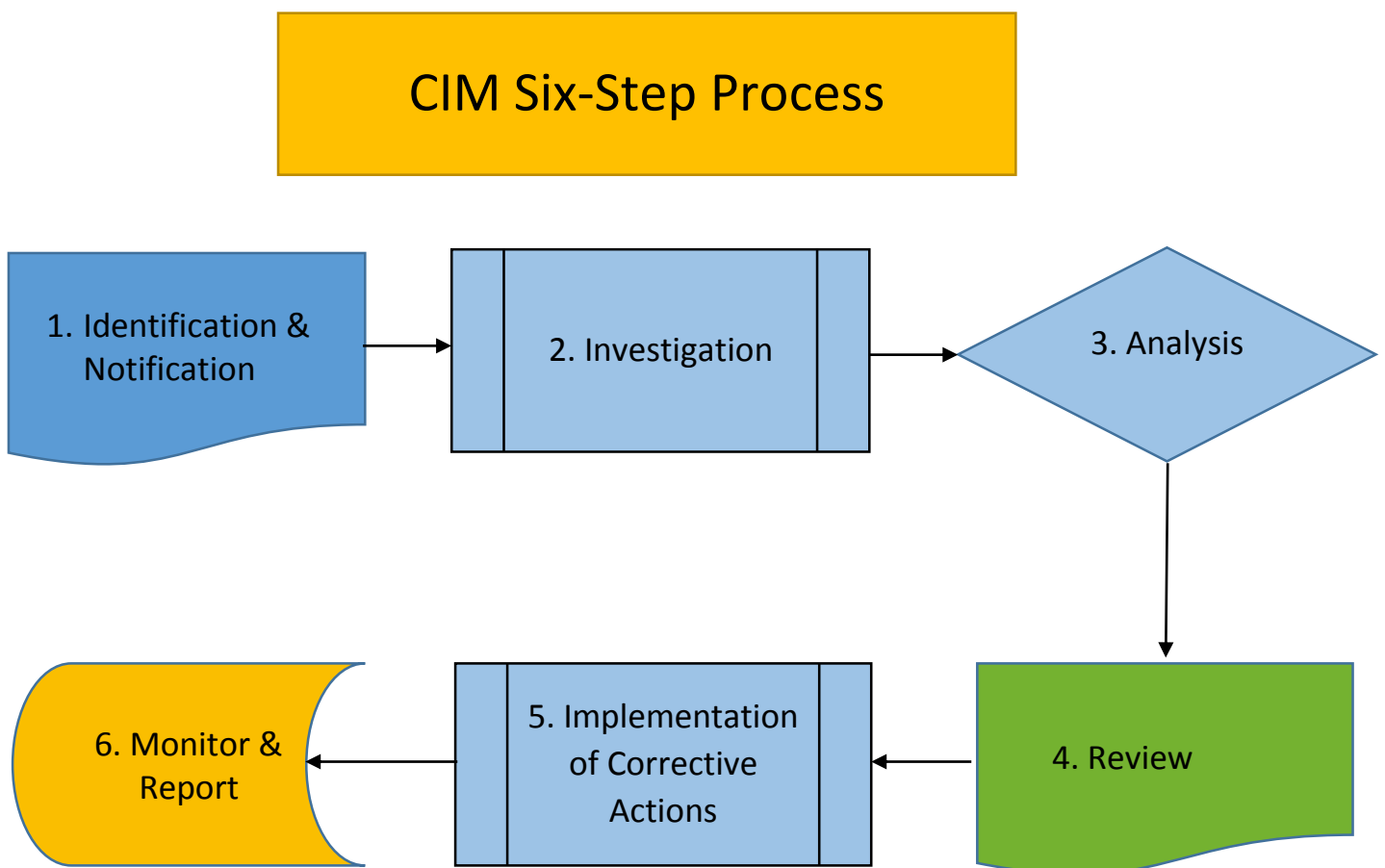
**Written Questions Taken on Notice – Medibank Health Solutions**

12.	MHS	A copy of the MHS Complaints protocol	Current
13.	MHS	MHS Privacy policies and procedures for: <ul style="list-style-type: none"><li>• First responders</li><li>• Trauma counsellors</li></ul> Including compliance and monitoring mechanisms.	Current

the following documents are attached:

- Item 12 - A copy of the MHS complaints protocol
  
- Items 13 & 14 – 1800 Respect Privacy Statement, Medibank Enterprise Security Policy, Medibank Code of Conduct, Medibank IT and Telecommunications Acceptable Use Policy and Medibank Privacy Policy.

## Complaints & Incident Management (CIM) Six-Step Process



### Purpose

The aim of Complaints & Incident Management (CIM) is to effectively manage reported complaints and clinical incidents (CIMS) with a view to reduce preventable patient or consumer incidents or issues.

### Process

There are six steps to effective CIM:

#### 1. Identification & Notification

It is important that all staff recognise the value the CIM process has in managing clinical risk and improving service quality. This is achieved in a culture and environment where CIMS are an acceptable part of service

delivery and an opportunity for improvement. Following identification there may need to be immediate action, which may include:

- Providing immediate care to individuals involved
- Making the situation safe to prevent recurrence of the event
- Removing malfunctioning equipment
- Gathering basic information, or
- Notifying ambulance or police or security

Staff are required to notify all identified CIMs via the RiskMan database located on the intranet. All actual CIMs must also be documented in the patient's case notes.

Notification must occur as soon as practicable and preferably is to occur by the end of the notifier's work day. The aim is to provide as much information as possible to assist with the investigation, review and management. A provisional (or initial) SAC rating is determined based on the information known at the time of lodgement.

## **2. Investigation**

Investigation is an important step of the process. Based on the level of risk, all submitted CIMs are screened and assigned for investigation by the CIM team. The investigation identifies what happened to cause the issue, staff involved and why it occurred. For adverse events, a root cause analysis may need to be conducted.

## **3. Analysis**

The analysis provides an understanding of how and why the incident occurred and identifies ways of preventing a recurrence. The analysis takes into account all the information gathered during the investigation phase and determines a root cause/s for the event. Recommendations are then made to prevent a recurrence.

## **4. Review**

A weekly review is conducted by a panel of internal clinical leadership staff and chaired by the delegated authority. This step reviews the results of steps 2 and 3 and discusses the investigation findings and conclusions. A final root cause and SAC rating are agreed upon. Corrective actions are also agreed upon, and they are assigned to appropriate staff along with a due date for completion.

## **5. Implementation of Corrective Actions**

This step includes putting into action the agreed plan for corrective action as determined in step 4, ensuring that timeframes are met.

## **6. Monitor and Report**

The CIM Manager is responsible for the monitoring and reporting of all submitted CIMs. This includes monitoring of all risks and issues to identify patterns and trends. Reports are provided to the:

- Client as contractually required
- Clinical Governance Committee, and
- Business level

<b>Site:</b>	Australia	<b>Created:</b>	16/07/12
<b>Department:</b>	PNIC Clinical Team	<b>Approved</b>	22/08/16
<b>Document No:</b>	APQRDQ191	<b>Last Updated:</b>	22/08/16
<b>Approved By:</b>	Chief Medical Officer	<b>Reviewed Only:</b>	

# 1800 RESPECT PRIVACY STATEMENT

## Who are we?

We are 1800RESPECT, the National Sexual Assault, Domestic and Family Violence Counselling Service which forms part of the National Plan to Reduce Violence against Women and their Children 2010-2022 (**Service**).

The Service is delivered by Medibank Health Solutions Telehealth Pty Limited ABN 40 069 396 792 (**MHS**), a subsidiary of Medibank Private Limited, on behalf of the Commonwealth of Australia through the Department of Social Services (**DSS**). In this privacy statement, references to 'us', 'we' and 'our' include DSS, MHS and any other contractors and service providers engaged in delivering the Service.

## Who does this privacy statement apply to?

This privacy statement applies to all individuals whose personal information we may collect in the course of providing the Service. This includes the people who contact us because they experience the impacts of sexual assault, domestic or family violence, family and friends affected by violence or abuse, and the frontline workers and professionals who use our resources to support people experiencing violence and abuse.

## Why do we collect personal information?

We are committed to protecting your privacy. You may use the Service anonymously or by using a pseudonym (that is, a fake name). However, it may not always be possible to provide you with all aspects of the Service anonymously or through using a pseudonym.

Where you provide us with personal information (that is, information about you or another person where you or that other person is identifiable) or where you have authorised another person to provide us with personal information, this information will be handled carefully and will be collected, used, stored and disclosed in a manner consistent with the *Privacy Act 1988*.

## What do we use personal information for?

We collect and use personal information to enable us to provide the Service and to meet our legal obligations. For example, we may use your personal information (where you choose to provide it) to provide you with online or telephone counselling services or to respond to your queries and feedback.

If you are a frontline worker or professional who supports people experiencing violence and abuse, we may use your personal information to:

- manage your registration to workers webinar series;
- provide you with frontline workers toolkit and resources;
- send you our workers and professionals newsletter;
- process and administer your requests to have your service listed;

- provide you with the tools, resources, and services we make available from time to time; and
- respond to your queries and feedback.

We may use de-identified information (where no one is identifiable) to improve the 1800RESPECT service, for reports and in evaluation of the Service and its various elements. De-identified information can also be used in academic articles and presentations at conferences.

We keep personal information only for as long as it is required in order to provide you with the Service and to comply with our legal obligations. When it is no longer needed for these purposes, we take reasonable steps to destroy or permanently de-identify it.

Any personal information held by MHS or its contractors and service providers in connection with the Service is held on behalf of DSS, so that we can provide the Service. If MHS stops providing the Service on behalf of DSS, and DSS requests, we will transfer the information to DSS or to such contractors as DSS appoints to perform the Service.

#### **Who do we disclose personal information to?**

The information may be shared between MHS, DSS and with contractors and service providers engaged to provide the Service (collectively, Contracted Service Providers). Where Contracted Service Providers are engaged, they are bound by obligations of security and confidentiality and contractual measures are in place to ensure they comply with those obligations.

We may disclose personal information to other persons where required to do so by law, such as to comply with mandatory reporting requirements in relation to suspected cases of child abuse and neglect.

De-identified information (where no one is identifiable) may also be shared with research partners.

#### **How do you access or correct personal information about you?**

We try to make sure that the personal information we collect, use and disclose is accurate, complete, up-to-date and relevant. You can request to access or correct personal information we hold about you. We will generally provide you with access to your personal information if practicable and will take reasonable steps to amend any personal information about you which is inaccurate or out of date. You can contact us by using the [Contact Us](#) page.

#### **Where can you get more information about our privacy practices?**

Our respective Privacy Policies contain more information about our privacy practices, including how you may request access to, or correction of, personal information we hold about you, how you can lodge a privacy complaint and how we manage such complaints. Whether your personal information has been collected by one of the below organisations will depend on which service you have used. If you would like more information, please contact us by using the [Contact Us](#) page.

You can obtain the latest version of our Privacy Policies by visiting our websites below:

- [Commonwealth Department of Social Services](#) (the funder of the service)

- [Medibank Health Solutions](#) (the coordinator of this service)
- [Rape and Domestic Violence Services Australia \(RDVSA\)](#) (who provide specialist counselling services)
- [TigerSpike](#) (the administrator of this website)
- [Real Time Health](#) (who provide online support tools and information for sector workers)
- [Redback Conferencing](#) (who provide the Workers Webinar service)
- [Survey Monkey](#) (a tool used to deliver online surveys)
- [Campaign Monitor](#) (a tool used to administer our campaigns and communications)

**This Privacy Statement is current as at April 2017 and may be updated from time to time.**

**Please consult this page regularly for any changes to the Privacy Statement.**

APPROVED



## Enterprise Security Policy

<b>Policy Level:</b>	L2
<b>Effective from:</b>	December 2015
<b>Document Owner:</b>	GM Security
<b>Date Approved:</b>	December 2015
<b>Approved by:</b>	DGM Technology & Operations
<b>Review Date:</b>	25 November 2015
<b>Version No.:</b>	6.0
<b>Status:</b>	Medibank in-Confidence
<b>Related Documents:</b>	Risk Management Policy; Procurement Policy; Medibank Business Continuity Policy; Information Security Organisation; Enterprise Security Standards; Code of Conduct; Privacy Policy; and IT&T Acceptable Use Policy.

## **1. PURPOSE:**

The protection of Medibank's assets is of extreme importance, an asset being a physical and/or virtual resource against which we place tangible value.

This document details enterprise-wide security policies which must be adhered to in order for Medibank to effectively protect our assets.

## **2. SCOPE:**

This policy is applicable to all Medibank staff, which includes paid and volunteer employees, third party contractors (service providers and consultants) and their employees, as well as any other party accessing Medibank's assets.

## **3. POLICY STATEMENT:**

It is Medibank's policy that we will protect the confidentiality, integrity and access to information in a predictable, consistent, measurable and effective manner in-line with applicable security good practices.

To fulfil our regulatory, legal, contractual and compliance obligations, we will:

- a) apply security in a pragmatic, tiered, business-centric and risk-based manner;
- b) ensure security augments our business strategy and objectives;
- c) effectively report, investigate and address actual or suspected violations of this policy; and
- d) provide suitable training will be provided to any party accessing a Medibank asset.

## **4. CONTROL FRAMEWORK**

A control framework has been employed for the purpose of managing our asset security risk to an agreed "acceptable business level".

This framework is based on the ISO 27000 series and includes specific requirements to cover our legal and legislative compliance obligations (e.g. PCI-DSS and the Australian Prudential Regulation Authority - APRA).

## **5. SECURITY ORGANISATION**

Security roles and responsibilities are clearly defined in our organisational structure.

## **6. SECURITY RISK**

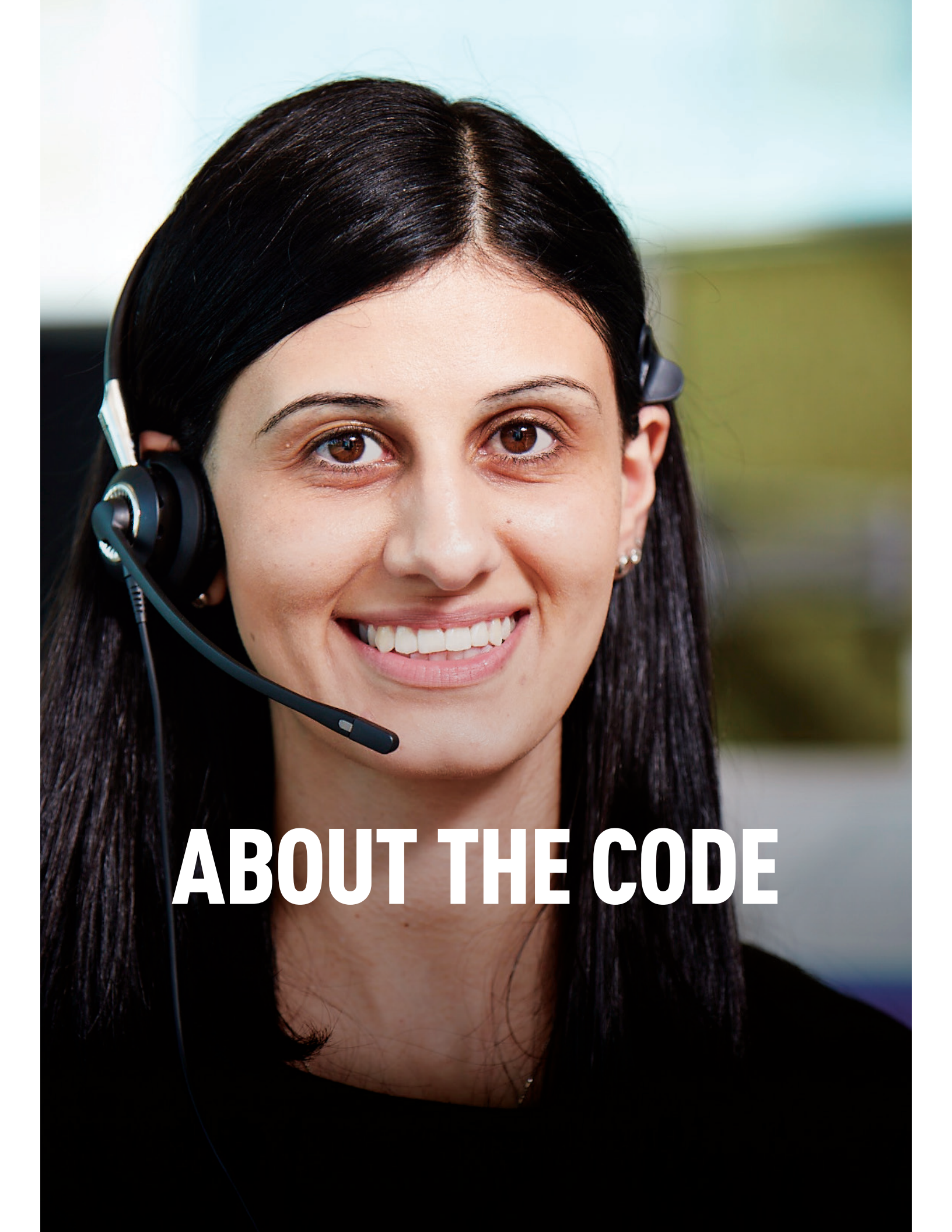
This policy supports the management of the internal and external sources of risk to information security i.e. the ability to protect the confidentiality, integrity and availability of information and information systems.

## **7. ADMINISTRATION**

This policy will be reviewed semi-annually or subject to significant organisational change.



# MEDIBANK CODE OF CONDUCT



**ABOUT THE CODE**

# SECTION 1

## ABOUT THE CODE

**As an organisation, we are committed to not only complying with our legal obligations, but also acting ethically and responsibly.**

### 1.1 What is the Code?

Our Code of Conduct sets out the way we work at Medibank. The Code sets out practical principles and minimum standards of behaviour and conduct which are expected of us, wherever we are and whoever we are interacting with – both within Medibank and with external parties.

The Code sets out our obligations in relation to:

- Law, standards and policy
- Health, safety and wellbeing
- Trust, accountability and transparency
- Conflicts of interest
- Anti-bribery and gifts
- Privacy and confidentiality
- Protection of assets
- Responsibility to the shareholders and the financial community
- Insider Trading

While the Code sets out minimum expectations of behaviour and conduct, it is not designed to be exhaustive. It cannot possibly cover every law, standard or Medibank policy that might apply to you.

As an organisation, we are committed to not only complying with our legal obligations, but also acting ethically and responsibly. We take the Code very seriously, so please make sure that you familiarise yourself with Medibank policies, procedures and guidelines that support the Code and are available on the intranet. You can refer to the Policy Addendum at the end of this document for guidance.

If you have any questions about the Code, speak to your People Leader or People & Culture (P&C) at any time.

### 1.2 Who does the code apply to?

The Code applies to anyone employed by or working

for Medibank. This includes the Medibank Board, employees (permanent, fixed term, fixed task and casual), contractors and consultants.

The Code applies to you whenever you are identified as a representative of Medibank. This may include occasions when you are outside your normal workplace or working hours, such as work functions, out of hours work activities, or when you are out in the community representing Medibank (e.g. a Community Leave day).

Wherever possible, Medibank will encourage its suppliers to comply with the Code of Conduct or adopt similar principles and policies.

### 1.3 What are my responsibilities as an individual?

- You are responsible for your own behaviour
- You are responsible for ensuring that you follow the Code
- You are responsible for speaking up if you see any behaviour that you think might breach the Code.

### 1.4 What are my additional responsibilities as a people leader?

- You are responsible for modelling best practice behaviour
- You are responsible for proactively dealing with breaches of the Code that you become aware of, including reporting them through the right channels where appropriate
- You are responsible for promoting a culture where employees, contractors and consultants understand their responsibilities; are encouraged to work in line with our Code and are encouraged to speak up about behaviour and conduct that is not in line with our Code.



# THE CODE

merit

Freedom of choice  
Peace of mind  
or better health

## SECTION 2

# THE CODE

**We foster relationships that are based on trust and respect. We are accountable and transparent in our dealings with our colleagues, our customers and our stakeholders.**

### 2.1 The law, standards and policy

At Medibank, we conduct our activities ethically and with integrity. This means we comply with any applicable laws, standards, and internal policies that are relevant to our roles and guide our conduct at work.

As an individual this means that you must:

- act with high standards of personal integrity
- not knowingly participate in any illegal or unethical activity
- be aware of the laws, standards and policies that apply to you and your job
- work in accordance with those laws, standards and policies
- undertake any training that is required of you in order to lawfully, safely and effectively do your job.


### 2.2 Health, safety and wellbeing

At Medibank, we're for better health. This means we take the health, safety and wellbeing of ourselves and others very seriously. Our objective is to prevent injury and illness. We are committed to supporting and maintaining a healthy and productive workplace that promotes the physical and psychological wellbeing of everyone within Medibank.

As an individual this means that you must:

- ensure your dealings with each other and with your clients, customers, suppliers, providers and other members of the public are free from bullying, harassment, discrimination and victimisation
- ensure your behaviour and conduct is in line with Medibank's expectations about the use of drugs, alcohol and tobacco in the workplace
- work in accordance with relevant Health, Safety and Wellbeing policies and procedures applicable to your role
- demonstrate safe behaviours and take reasonable care for your own health and safety, and the health and safety of others
- report incidents and hazards observed in your workplace and, where possible, make the area safe for others.





**“ At Medibank, we conduct our activities ethically and with integrity.”**

### 2.3 Trust, accountability and transparency

We foster relationships that are based on trust and respect. We are accountable and transparent in our dealings with our colleagues, our customers and our stakeholders.

As an individual this means that you must:

- act honestly, in good faith and in the best interests of Medibank
- display skill, professionalism, care and diligence in your duties
- present for work in appropriate attire
- treat your colleagues, customers, suppliers, providers and other members of the public with courtesy and respect at all times
- respect diversity and individual differences
- respect the property of Medibank and of others
- comply with all reasonable and lawful instructions given by a people leader or other authorised person
- not make false representations in connection with your employment
- not take any improper advantage of your position or any information available to you, including for your personal gain, or where it would cause detriment to Medibank or its customers
- only provide information about Medibank’s products to consumers if you are authorised and trained by Medibank to provide such advice
- use social media ethically and responsibly
- be fair in all dealings with competitors
- make sure you do not engage in any anti-competitive behaviour or conduct, including, but not limited to, discussing and exchanging pricing or marketing information with competitors.

## 2.4 Conflicts of interest

At Medibank, we understand the importance of identifying and effectively managing conflicts of interest. We never put ourselves in a situation that puts, or appears to put, our own personal interests before those of Medibank or our customers. We also understand that a perceived conflict of interest should be treated with as much care as an actual conflict of interest.

A conflict of interest may occur when personal interests or activities influence, or could appear to influence, your ability to act in the best interests of Medibank. Examples of a personal interest include a financial gain, a professional advancement or advancement for yourself, a family member or a friend.

They may relate to:

- employment outside of Medibank
- investments in a competitor or supplier
- serving as a director of another business.

As an individual this means that you must:


- avoid any actual, potential or perceived conflicts of interests between your personal or outside interests, as well as the interests of Medibank, its customers, suppliers and members
- not enter into any arrangements or participate in any activity that would conflict with Medibank's best interests or that would be likely to negatively affect Medibank's reputation
- raise any conflicts with your People Leader or P&C Business Partner. Alternatively, you can use the Whistle-blower Procedure if appropriate
- obtain approval from a relevant People Leader for any outside business interests with the potential to create a conflict, or the appearance of a conflict.

## 2.5 Anti-bribery and gifts

At Medibank, we have a strict policy prohibiting employees from offering or accepting secret commissions or bribes to further Medibank's business interests. Care must be exercised in accepting hospitality, entertainment or gifts over and above that required for the normal conduct of business or which may compromise your impartiality. In addition, receiving a gift or benefit may create, or appear to create, a conflict of interest.

As an individual this means that you must:

- not accept any money or opportunity or other benefit which could be interpreted as an inducement, secret commission or bribe
- only accept gifts or benefits if they are provided as part of an approved incentive program
- not accept gifts, hospitality, entertainment or anything of value that might have or appear to have obligations attached
- not offer or give anything of value, or solicit any inducement, that may conflict with your work or your duties to Medibank
- ensure any approved grants or donations to charities or organisations made on behalf of Medibank are recorded in Medibank's register for gifts, entertainment, grants and donations
- not support or assist a political organisation, a member of a political organisation or a political candidate in your capacity as a representative of Medibank
- not support, make or offer any grants, donations, or facilitate payments to any political organisations or associated groups, government officials, government employees or contractors, or private parties in your capacity as a representative of Medibank.



**“ We understand that a perceived conflict of interest should be treated with as much care as an actual conflict of interest.”**

## 2.6 Privacy & confidentiality and protection of assets

At Medibank, we respect the privacy and confidentiality of our colleagues, members, clients, customers, suppliers and service providers. We understand that Medibank owns the property rights to all information, goods or services generated during the course of employment.

As an individual this means that you must:

- ensure that information is collected, kept, disclosed, handled and used in a manner that complies with the Privacy Act 1988 (Cth), and any other privacy and data protection laws that may apply
- keep all personal information of our customers private and confidential
- maintain the security of information and protect it from unauthorised use, access, modification and disclosure
- only access our customers' information if you are trained and authorised to do so
- not discuss or disclose the personal or private information of your colleagues, consultants, contractors or service providers
- only disclose information relating to colleagues, consultants, contractors or service providers where authorised and/or if required by law
- maintain the confidentiality of information, including commercial information, of Medibank and other relevant parties
- keep all information gained during the course of your employment confidential, unless required by law to disclose it
- not discuss or disclose information relating to Medibank, our Group Companies or our employees, contractors or consultants without the proper authority to do so
- only use the resources of Medibank and our system access in the course of normal duties
- not use or misuse Medibank's assets, systems, confidential information or intellectual property, to gain an improper advantage or benefit
- not infringe the intellectual property rights of Medibank or others.



## 2.7 Responsibility to the shareholders and the financial community

At Medibank, we are committed to promoting investor confidence and the rights of shareholders and other stakeholders by complying with Medibank's continuous disclosure obligations. Medibank has policies regarding the timely provision of information to our shareholders and other stakeholders including posting information to our website. We have processes to ensure that the accounts and financial information we provide represent a true and fair view of the financial performance and position of Medibank.

As an individual, this means that you must:

- not discuss or make comments about Medibank's business or operations that is not public information to any person or forum outside Medibank without authorisation, including via the internet, on social media or social networking sites; and
- fully cooperate with, and not make any false or misleading statement to, or conceal any relevant information from, Medibank's auditors.

## 2.8 Insider trading

At Medibank, we have a strict policy on share trading. Insider trading laws prohibit a person in possession of material non-public information relating to a company from dealing in that company's securities. Insider trading is a serious offence under the Corporations Act.

As an individual, this means that you must:

- familiarise yourself with Medibank's Share Trading Policy
- ensure that you do not deliberately or inadvertently breach the insider trading laws or Medibank's Share Trading Policy.

# DEALING WITH BREACHES OF THE CODE



## SECTION 3

# DEALING WITH BREACHES OF THE CODE

**Medibank will ensure, as far as possible, that anyone who reports a breach of the Code in good faith is given confidentiality and ongoing support through the process.**

### 3.1 How do I raise a concern?

You can speak to your People Leader in the first instance. They will work with you to address the concern you've raised and seek necessary advice from a senior leader or a P&C Business Partner if required.

If there's a reason you are not able to raise your concern directly with your People Leader, you can speak with your Senior Leader (this is usually the person your People Leader reports to) or contact your P&C Business Partner directly for advice.

If you are not able to use the options above, you may choose to use Medibank's Whistle-blower Procedure (Medibank Alert) which allows you to report conduct anonymously, or limit who is informed of your identity. Contact Medibank Alert on 1800 453 411.

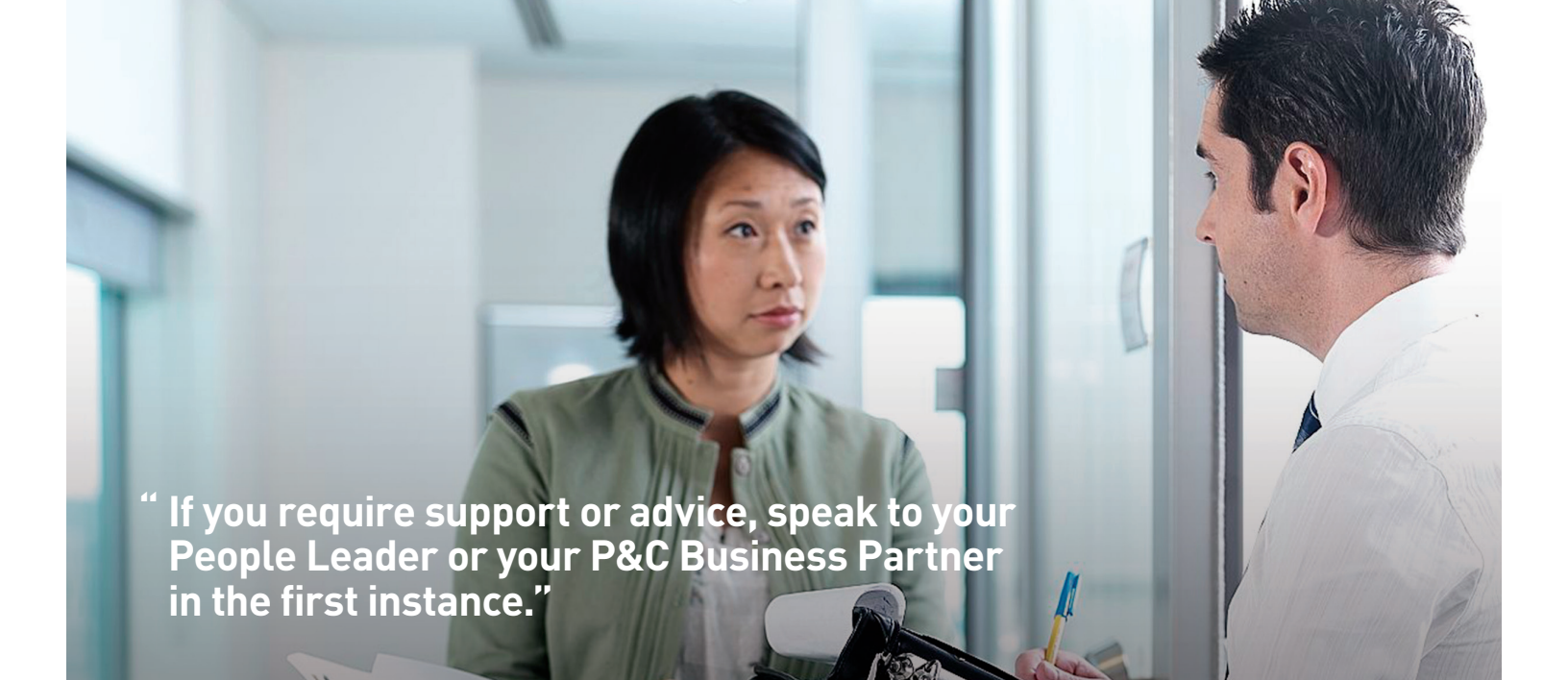
### 3.2 What happens if I breach the code?

There are different options for dealing with a breach of the Code depending on the circumstances:

- A conversation may occur between you and your People Leader
- A conversation may occur between you and a member of the P&C team
- An investigation might be undertaken in relation to the breach
- In the most serious cases, there may be an external investigation and/or involvement of the Legal team.

Where it is determined that a breach has occurred, the severity, intent and impact of the breach will be taken into account and any of the following actions may be taken:

- The issue may be managed locally by the People Leader
- You may be required to attend training or counselling
- You may be subject to a performance management process
- You may be subject to disciplinary action (which can include warnings or termination of employment).



**“ If you require support or advice, speak to your People Leader or your P&C Business Partner in the first instance.”**

### 3.3 What do I do if someone reports a breach of the code to me as a people leader?

You need to listen to the concern that has been raised and assess the severity of the alleged breach. Ask yourself:

- Does this have an impact on my team?
- Does this have an impact on the organisation?
- Does this have any legal implications?
- Are there any reputational risks for the business?
- Is this likely to generate negative publicity for Medibank?
- Is anyone’s health and safety at risk?

Your answers will help guide what you do next. Options could include:

- managing it locally (e.g. it’s an interpersonal conflict between two or more individuals)
- seeking advice and support from your P&C Business Partner, your senior leader or other appropriate channels (e.g. this issue may need to be investigated and may have disciplinary outcomes for one or more employees)
- reporting the breach through the appropriate Incident Management System.

### 3.4 What support is available to me?

Medibank will ensure, as far as possible, that anyone who reports a breach of the Code in good faith is

given confidentiality and ongoing support through the process. Similarly, anyone who is alleged to have breached the Code will be given fair and reasonable opportunity to respond to any concerns raised and will be supported through the process.

Medibank does not tolerate victimisation and will take appropriate action against anyone found guilty of this.

You are also encouraged to use the Employee Assistance Program (EAP). This program is free, confidential and available 24 hours a day for our employees and members of their immediate family to seek advice, support and counselling for personal and professional issues. Contact the EAP on **1800 808 374** at any time.

If you are a People Leader, the EAP offers a Manager Support Program (MSP) to provide you with advice and support. Contact the MSP on **1800 505 015** at any time.

### 3.5 Where do I get more information?

At the end of this document you will find the Policy Addendum, which lists relevant policies that underpin the Code of Conduct and provide more detailed information on areas covered in the Code.

Please read the relevant policies to understand your obligations and those of others.

If you require further information or have any queries, you should speak to your People Leader or your P&C Business Partner in the first instance.



## Policy Addendum

Code of Conduct section reference	Relevant internal policy
All sections	<ul style="list-style-type: none"> <li>Whistleblower</li> <li>Risk Management</li> <li>Performance Management and Conduct</li> </ul>
2.2 Health, Safety and Wellbeing	<ul style="list-style-type: none"> <li>Health, Safety and Wellbeing</li> <li>Bullying, Harassment and Discrimination (Unacceptable Behaviour)</li> <li>Drugs, Alcohol and Tobacco</li> </ul>
2.3 Trust, Accountability and Transparency	<ul style="list-style-type: none"> <li>Diversity</li> <li>Social Media</li> <li>Fraud</li> </ul>
2.4 Conflict of Interest	<ul style="list-style-type: none"> <li>Conflict of Interest</li> <li>Giving and Receiving Gifts</li> </ul>
2.5 Anti-bribery and Gifts	<ul style="list-style-type: none"> <li>Anti-bribery and Anti-corruption</li> <li>Conflict of Interest</li> </ul>
2.6 Privacy and Confidentiality	
2.7 Responsibility to Shareholders and the Financial Community	<ul style="list-style-type: none"> <li>Disclosure and Communication</li> <li>Social Media</li> </ul>
2.8 Insider Trading	<ul style="list-style-type: none"> <li>Share Trading</li> </ul>
3.1 How do I raise a concern?	<ul style="list-style-type: none"> <li>Bullying, Harassment and Discrimination (Unacceptable Behaviour)</li> <li>Whistle blower</li> </ul>
3.2 What happens if I breach the Code?	<ul style="list-style-type: none"> <li>Performance Management and Conduct</li> </ul>
3.4 What support is available to me?	<ul style="list-style-type: none"> <li>Performance Management and Conduct</li> <li>Health, Safety and Wellbeing</li> <li>Bullying, Harassment and Discrimination (Unacceptable Behaviour)</li> <li>Employee Assistance Program</li> </ul>

Please note: this addendum is designed to help guide you in the direction of some key policies that are relevant to the Code. There may be other documents that are not listed here that are also relevant to you and the work that you do in Medibank. You have a responsibility, as far as is reasonable, to familiarise and educate yourself on the obligations you have in your role within Medibank.

This policy was updated in October 2014.



# IT and Telecommunications Acceptable Use Policy v4.0

## Introduction

As a Medibank employee and authorised user, you are granted access to Medibank information assets and the systems that store and process that information. With this access comes a set of obligations which you and all users must acknowledge and adhere to.

These obligations are set out below as the:

**Medibank IT and Telecommunications Acceptable Use policy.**

## Applicability

This policy is applicable to all staff of Medibank, which includes paid and volunteer employees, third party contractors (service providers and consultants) and their employees, as well as any other persons who have access to Medibank's information systems or data.

This policy applies to the use of all IT&T Resources, defined as all IT and telecommunications equipment or resources owned or provided by Medibank, or its contracted third party providers, including desktop and lap-top computers, information systems, software, wireless data cards, land-line phones, mobile phones and tablets.

## Effective Date

April 2015

## Policy Review

Medibank will review and may change this policy periodically. Any changes will be communicated to staff.

## Policy Owner

Ultimate ownership of this policy rests with the Board of Medibank and the Executive Management Team.

IT and P&C are jointly responsible for overseeing the application of this policy.

IT are responsible for the technical aspects (e.g. logging and monitoring) associated with this policy. P&C are responsible for supporting it through Medibank's other relevant policies and codes of conduct.

If you have any questions about this policy you should contact your line manager, P&C Rep or the Help/Service Desk.

## Underlying Principle

The key principle that underpins the Acceptable Use policy is that Medibank is committed to enabling its people (including employees, contractors and third party providers) to perform their work effectively, safely and securely, in both Medibank offices and remote locations.

## Guiding Objectives

Users of Medibank IT&T Resources should not do anything with the facilities which may:

- Interfere with the operation of IT and communications facilities;
- Waste Medibank IT&T Resources;
- Interfere with the work performance of other people;
- Be offensive or be likely to offend;
- Create a risk to health and safety of other people;
- Expose Medibank to legal action or public criticism;
- Expose Medibank to commercial and/or financial loss.

## Access Revocation

Medibank allows authorised users to access IT&T Resources governed by this policy, until authorisation is revoked. Once a user has been advised that authorisation has been revoked, the user must not access IT&T Resources even though the ability to access those facilities may not yet have been removed.

## Acceptable Use

“Acceptable use” of IT&T Resources encompasses:

- The performance of authorised business activities for Medibank.
- Bona fide work-related self-improvement and professional development activities.
- Limited reasonable personal use that does not otherwise breach this policy, interfere with or adversely impact upon the operation of Medibank.

## Unacceptable Use

Without being exclusive the following is considered unacceptable use of IT&T Resources:

- Attempted or actual access, transmission, storage or possession of pornography or any material that is illegal, unethical, offensive, discriminatory, in breach of copyright or licensing conditions, or which may reasonably be regarded as objectionable.

**Note: Being able to access material of this nature does NOT indicate that the relevant material is exempt from this policy.**

- Attempted or actual unauthorised access, transmission, storage or possession of commercially confidential, market-sensitive, personally-identifiable, personal health, or payment card information or data, including but not limited to:
  - Attempted or actual storage or possession of unencrypted sensitive information on local hard drives or removable media.
  - Attempted or actual access, storage, copying, or moving of unencrypted sensitive information when accessing the data via remote-access technologies.
  - Transmission of unencrypted sensitive information in e-mail or other communication forms such as instant messaging or unsecured fax.
  - Attempted or actual access, transmission, or storage of hoax, junk or spam email. (continued...)



## Unacceptable Use (continued)

- Attempted or actual access, transmission, storage or possession of malicious code or programs which affect the functionality or security of IT&T Resources.
- Any activity involving IT&T Resources that breaches any other Medibank policy.
- Conducting unlawful or unethical activities.
- Revealing your account password to others or allowing use of your account by others.
- Attempted or actual unauthorised access of IT&T Resources by using the User ID and/or Password assigned to another person.
- Installing new software or modifying existing software or security controls without authorisation.
- Unauthorised non-work related activities such as fundraising, religious or political activities.
- Conducting private business or other activities for personal or financial gain.
- Access or use of any IT&T Resources to which authorisation has not been granted.

## Monitoring

Users should understand that Medibank is the owner of all IT&T Resources including, equipment, software and data transmitted or received. As such, Medibank monitors use of IT&T Resources including internet and email activities, file servers and workstations, and can do so at any time and without user consent.

Electronic mail that may breach Medibank usage policies is stored in a database with relevant details, including user email address, content and attachments. This database is accessed by Medibank for investigative purposes.

Under certain circumstances, reports may be provided to authorised personnel who wish to receive statistics on their employee's internet usage.

Intrusion detection systems have been installed to alert Medibank when attempts are made to gain unauthorised access to computer systems, exploit security weaknesses or perform any malicious activity.

This monitoring should not be relied upon to identify all unacceptable material or activities and therefore is not meant to replace any of your duties under these guidelines.

## Securing Equipment

You must minimise the chance of unauthorised access to your assigned IT&T Resources if you leave any of these devices unattended.

## Duty To Ensure Compliance

Where you believe that a person has breached this policy the matter should be immediately referred to your line manager, P&C Rep or the Help/Service Desk.

### Consequences of Breach of Policy

The legal and commercial risks that may impact on Medibank as a consequence of a breach of the guidelines are very real. Users found to be in breach of this policy may face a range of repercussions including:

- A written warning; and/or counselling/coaching;
- Suspension or withdrawal of facilities or resources.

A serious breach may result in further sanctions including:

- Termination of employment; criminal or civil legal action.

### Related Policies

This policy is to be read and applied in conjunction with other Medibank policies, standards and guidelines including:

- Code Of Conduct
- Social Media Policy
- Information Security Policy

In the event of any discrepancy between the requirements imposed by different policies, the more stringent security requirement is to be applied.

## Definitions

### IT&T

Information Technology and Telecommunications.

### Authorised users

Those individuals who have been authorised to access one or more particular IT&T Resource by the appropriate line manager. An individual is an "Authorised User" for only those approved IT&T Resources.

## Document Control

Revision History	Date	Comments	Compiled By	Approved By
Ver 1.0	Oct 2010	Original	IT Security	ITLT
Ver 1.1	Nov 2011	Annual Review	Information Security	ITLT
Ver 2.0	Apr 2013	Format Change	Information Security	GE
Ver 2.1	July 2013	Minor Changes for MHS Rollout	Information Security	MHS
Ver 2.2	Aug 2013	Annual review and minor update	Information Security	GE
Ver 3.0	Apr 2014	Moved to Final	Information Sec. Gov.	GE
Ver 3.1	Nov 2014	Annual review – no change	Information Sec. Gov.	
Ver 4.0	Jan 2015	Made Final	Information Sec. Gov.	GE

# MEDIBANK PRIVACY POLICY

March 2014

**medibank**  
For Better Health

## Who are we?

We are Medibank Private Limited ABN 47 080890 259 (**Medibank**) and Australian Health Management Group Pty Ltd ABN 96 003 683 298 (**ahm**), a subsidiary of Medibank. References to 'us', 'we' or 'our' include Medibank, ahm and, where the context requires, other Medibank subsidiaries (collectively **Medibank Group Companies**).

## Who does this policy apply to?

This privacy policy applies to:

- All current and past members of Medibank and ahm whose personal information we have collected
- All individuals whose personal information is collected in relation to the products and services offered by Medibank Group Companies
- All individuals whose personal information is collected by us in the course of our functions and activities such as service providers, contractors and prospective employees.

## Protecting your privacy

We are committed to protecting your personal information and complying with our obligations under the *Privacy Act 1988* (Cth) (Privacy Act) and other State and Territory laws governing the use of personal information (collectively, **Privacy Laws**) which regulate how personal information is handled from collection to use and disclosure, storage, access and disposal.

'Personal information' generally means any kind of information in any form about a person that identifies that person and includes sensitive information such as health information.

This privacy policy explains:

- how we manage the personal information that we collect, use and disclose; and
- how to contact us if you:
  - have any questions about our management of your personal information; or
  - would like to access or correct the personal information we hold about you; or
  - would like to lodge a complaint with us regarding our compliance with Privacy Laws.

## What kind of personal information do we collect?

The types of personal information we may collect include:

- identifying information such as name, date of birth and employment details;
- contact information such as home address, home and mobile phone numbers and email address;
- government-issued identifiers including Medicare numbers;
- financial information, such as bank account and credit card details;
- sensitive information, including information about your health, health services provided to you and your claims;
- biometric information and templates, such as voice recognition information;
- information about your activities, including sporting and other lifestyle interests; and
- information about involvement in other programs you participate in or memberships you may have.

You generally have the right not to identify yourself when dealing with us where it is lawful and practicable for us to allow it. However, on many occasions we will not be able to do this. For example, we will need your name and residential address in order to provide you with private health insurance coverage.

If you do not provide or authorise the provision of personal information we request, we may be unable to provide you with some or all of our products and services or the product and services of our partners.

By becoming or remaining a member of one of our policies or by otherwise providing personal (including sensitive) information to us, you confirm that you and other members covered under the policy or other individuals whose information you or they provide have consented to us collecting, using and disclosing your and their personal (including sensitive) information, however collected by us, in accordance with this privacy policy.

## How do we collect and hold your personal information?

We will only collect personal information about you by lawful and fair means and not in an unreasonably intrusive manner.

We may collect your personal information from:

- you, another person covered by your policy or from a person authorised to provide us this information on your behalf;
- a third party such as a hospital, dentist or optometrist or other health service provider who has treated you;
- an employer, educational institution, government agency or adviser who has dealt with you (or their authorised representatives);
- Medibank Group Companies who have provided you with services including health-related services;
- a service provider engaged by us or a third party who partners with us; and
- another health fund, if you are looking to transfer your membership.

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

We store your information securely and have a range of security controls in place to ensure that your information and documents are protected. Our employees are trained on privacy and access to personal information is restricted to individuals properly authorised to do so.

We also take reasonable steps to make sure that the personal information that we collect, use and disclose is accurate, complete, up to date and relevant.

We keep your personal information for only as long as it is required in order to provide you with products and services and to comply with our legal obligations. When it is no longer needed for these purposes, we take reasonable steps to destroy or permanently de-identify this personal information.

## Why do we collect, use and disclose your personal information?

### Collection

We **collect** your personal information to enable Medibank Group Companies and our third party suppliers and partners to provide you with products and services, including insurance, health-related services, partner offerings and information on other products and services (collectively **Insurance and Health Products**). We may also be required by law to collect some personal information.

Where you provide personal information to the Medibank Group Companies as a service provider, contractor or prospective employee, we collect your personal information to enable us to fulfil the purpose and related purposes for which you provided the information.

### Use

We may **use** your personal information for these purposes, including to:

- process your policy application and manage your policy;
- manage our relationship with you;
- process and audit payments and claims;
- analyse, investigate, pursue and prevent suspected fraudulent activities;
- manage and develop Insurance and Health Products;
- assess your suitability for and contact you about Insurance and Health Products that we believe may be of benefit to you;
- partner or work with third parties to improve our membership offering and value;
- manage and develop our business and operational processes and systems;
- conduct marketing, feedback and research activities;
- manage and resolve any legal or commercial complaints or issues;
- perform other functions and activities relating to our business; and
- comply with our legal obligations.

## Disclosure

In doing so we may **disclose** your personal information to persons or organisations in Australia and overseas including:

- our subsidiaries;
- our agents and service providers;
- our professional advisors;
- health service providers;
- other persons covered by your policy as part of administering the policy and paying benefits;
- potential or actual buyers of our assets, business or of shares in Medibank Group Companies;
- payment system operators and financial institutions;
- your agents and advisors or other persons authorised by, or responsible for, you;
- government agencies;
- your educational institution, migration agent or broker if you have OSHC or a visitors cover product;
- third party insurers whom we are authorised to represent if you purchase other insurance products through us;
- third parties with whom Medibank partners or works with to improve its membership offering and value;
- other health funds, service providers or other third parties who assist us in the detection and investigation of fraud;
- your employer (or their authorised representatives) if you have a corporate insurance product; and
- other parties to whom we are authorised or required by law to disclose information.

## How we communicate with you

To keep you informed quicker, where you provide us with an email address, we send most service-related communications to you by email. Service-related communications are the essential things you need to know about your cover, like annual tax statements, changes to premiums and account notices.



From time to time, we may also collect and use your personal information so that we can promote and market Insurance and Health Products to you and keep you informed of special offers from Medibank Group Companies and third parties, including by direct mail, SMS and MMS messages, by phone and email.

You can choose how we communicate with you and manage your consents to receiving promotions and offers by contacting us:

**Medibank:** Access the Manage My Preferences page within the Medibank Online Member Services facility, call us on 132 331 or visit one of our stores.

## **How is your information managed when you receive health-related services from us?**

This section of our Privacy Policy applies only to health-related services provided to our private health insurance members by Medibank Health Solutions (**MHS**), a division of Medibank. MHS may provide such services to our private health insurance members including telephonic services, chronic disease and health management programs and online health-related services.

MHS may collect and use your personal information to provide these services to you including to:

- manage their relationship with you and contact you for follow up purposes;
- manage, review, develop and improve their health-related services and their business and operational processes and systems;
- resolve any legal and/or commercial complaints or issues; and
- perform any of their other functions or activities as described within the MHS Privacy Policy.

MHS may collect your personal information from another Medibank Group Company, from you or from a person authorised by or responsible for you.

If you use health-related services, MHS may disclose your personal information to Medibank or ahm in order for us to pay benefits for health-related services and to review, develop and improve the services.

In order to perform the above functions, MHS companies may disclose your personal information to each other and to third parties such as their agents, service providers and professional advisors, health service providers, persons authorised by or responsible for you, and to other parties to whom they are authorised or required by law to disclose information including government agencies, and these parties may collect that information.

Medibank Group Companies may also use and disclose your personal (including sensitive) information to each other:

- to assess from what other services you may benefit and to facilitate the provision of such services
- so we may have an integrated view of our members and provide you a better and personalised service; and
- to contact you (including by telephone call, text message or email) in relation to our health-related services.

You may withdraw your consent to the sharing of your sensitive information between Medibank Group Companies or to being contacted in relation to our health-related services by contacting us:

**Medibank:** Access the Manage My Preferences page within the Medibank Online Member Services facility, call us on 132 331 or visit one of our stores.

For further information about how your personal information is handled for these health-related services, please refer to Medibank Health Solutions' Privacy Policy on the website at [www.medibankhealth.com.au](http://www.medibankhealth.com.au)

## **Do we disclose your personal information overseas?**

We may need to disclose your personal information to organisations located outside of Australia from time to time in the ordinary course of our business. Most of these overseas organisations are services providers or related entities which provide support and assistance to us in delivering our products and services to you.

Where we do, we take reasonable steps to ensure that your information is given the same type of protection as it is afforded within Australia. This may be through satisfying ourselves that the overseas organisation has controls in place to comply with Australian privacy laws, ensuring that the overseas organisation is located in a country which we believe has a similar privacy regime to Australia or through contractually or otherwise mandating the adequate management of the information.

On occasion, we may also disclose your personal information to overseas organisations where you instruct us or expressly consent to us doing so. In such cases, we may not take the above steps in relation to the management of your information.

If you have a corporate health insurance product, there may be occasions where we are instructed by your employer to disclose your information to an overseas organisation in order to administer your policy. In such instances, we may not be able to take reasonable steps to ensure that your information will be afforded the same protection as in Australia and you may not be able to seek redress for how your information is handled under Australian privacy law.

Please see at the end of this policy which outlines the main countries to which personal information may be disclosed.

### **You can access or correct your personal information. How do you contact us to do so?**

We will generally provide you with access to your personal information if practicable (although an administration fee may be charged), and will take reasonable steps to amend any personal information about you which is inaccurate or out of date.

You can get in touch with us at Medibank to request the above any time you wish to do so.

In some circumstances, we may not permit access to your personal information, or may refuse to correct your personal information. Where this happens, we will provide you with reasons for this decision, seek alternatives and take any further legally required steps.

## **Do you have any concerns over the way we have collected, used or disclosed your personal information?**

If you have any concerns or queries about the manner in which your personal information has been handled, please contact our Privacy Officer whose contact details are provided below.

If you wish to make a formal complaint, please provide your complaint in writing to our Privacy Officer. We will consider your complaint promptly and contact you to seek to resolve the matter.

Generally, we will contact you to acknowledge receipt of your complaint and let you know who is managing your query within 5 business days. We will attend promptly to your complaint and will aim to respond to your concerns or otherwise keep you informed of our progress within 30 days.

If we have not responded to you within a reasonable time or if your complaint is not resolved to your satisfaction, you are entitled under the Privacy Act to make a complaint to the Office of the Australian Information Commissioner.

**Medibank:** Privacy Officer, Medibank Private Limited, 16/700 Collins Street, Docklands, VIC 3008 or e-mail [privacy@medibank.com.au](mailto:privacy@medibank.com.au)

## **Further information**

Further information about the application of the Privacy Act can be found at the website of the Office of the Australian Information Commissioner at [www.privacy.gov.au](http://www.privacy.gov.au).

## **Changes to our Privacy Policy**

This privacy policy was last reviewed in March 2014. As this privacy policy is updated from time to time, to obtain a copy of the latest version at any time, you should visit our website at [www.medibank.com.au](http://www.medibank.com.au)

## Countries to which personal information may be disclosed

Listed below are the countries to which we may disclose personal information in the course of our functions and activities. This list does not include countries where you may have specifically instructed us to send your information or expressly consented to us sending your information.

Please see the **Do we disclose your personal information overseas?** section for information on the steps we take to ensure the adequate protection and appropriate management of this information.

- India
- New Zealand
- United States

This list is updated from time to time. You can visit our website at any time to view the latest version.

**ask in store  
visit [medibank.com.au](https://www.medibank.com.au)  
or call 132 331**

**medibank**  
For Better Health

The information contained in this brochure supersedes all previously published material.  
Medibank Private Limited ABN 47 080 890 259 MPL30830314