Disclaimer
This publication may contain occupational health and safety and workers compensation information. It may include some of your obligations under the various legislations that WorkCover NSW administers. To ensure you comply with your legal obligations you must refer to the appropriate legislation.

Information on the latest laws can be checked by visiting the NSW legislation website (www.legislation.nsw.gov.au) or by contacting the free hotline service on 02 9321 3333.

This publication does not represent a comprehensive statement of the law as it applies to particular problems or to individuals or as a substitute for legal advice. You should seek independent legal advice if you need assistance on the application of the law to your situation.

© WorkCover NSW
CONTENTS

PREFACE 2
Abbreviations used 2
Glossary 2

CHAPTER 1 – INTRODUCTION 3
1.1 Background – Why we have a Privacy Management Plan 3
1.2 Scope – What is in our Privacy Management Plan 3
1.3 Statutory Requirements – What laws impact on the activities of WorkCover 3
1.4 Legislation – What laws impact on how WorkCover manages information 4
1.5 Privacy Codes of Practice – Public Interest Directions 7
1.6 WorkCover External Data Release Policy 7

CHAPTER 2 – PRIVACY MANAGEMENT POLICY 8
2.1 Policy – Our commitment to information privacy 8
2.2 Compliance – How we meet the Information Protection Principles 12
2.3 Public Register – How we comply with the Public Register provisions 15
2.4 Continuous Improvement – How we improve what we do 16
2.5 Reporting – How we let people know about information management 17

CHAPTER 3 – PRIVACY MANAGEMENT PROCEDURES 18
3.1 Information – What significant personal information is held by WorkCover 18
3.2 How WorkCover manages personal information 23
3.3 How WorkCover manages access to and amendment of personal information 23
3.4 How WorkCover manages complaints about its conduct under the Privacy and Health Records Acts 24
3.5 How WorkCover will disseminate privacy policies and related information 25
PREFACE

ABBREVIATIONS USED

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>OHS Act</td>
<td><em>Occupational Health and Safety Act 2000 (NSW)</em></td>
</tr>
<tr>
<td>Privacy Act</td>
<td><em>Privacy and Personal Information Protection Act 1998 (NSW)</em></td>
</tr>
<tr>
<td>Health Records Act</td>
<td><em>Health Records and Information Privacy Act 2002 (NSW)</em></td>
</tr>
<tr>
<td>State Records Act</td>
<td><em>State Records Act 1998 (NSW)</em></td>
</tr>
<tr>
<td>WC &amp; WOHS Council</td>
<td><em>Workers Compensation and Workplace Occupational Health and Safety Council</em></td>
</tr>
</tbody>
</table>

GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkCover</td>
<td>Unless specifically identified, WorkCover refers to:</td>
</tr>
<tr>
<td></td>
<td>• WorkCover NSW Board of Directors</td>
</tr>
<tr>
<td></td>
<td>• Office of the WorkCover Authority</td>
</tr>
<tr>
<td></td>
<td>• WC &amp; WOHS Council</td>
</tr>
<tr>
<td></td>
<td>• Workers Compensation Insurance Fund Investment Board</td>
</tr>
<tr>
<td>Personal Information</td>
<td>Personal information is information or an opinion about a person who can be identified from the information. Depending on the circumstances, this can include person’s name, date of birth, address, telephone number, family members, or any other information that could allow the person to be identified.</td>
</tr>
<tr>
<td>Health Information</td>
<td>Health information includes personal information that is information or an opinion about:</td>
</tr>
<tr>
<td></td>
<td>• the physical or mental health or a disability (at any time) of an individual;</td>
</tr>
<tr>
<td></td>
<td>• a health service provided, or to be provided, to an individual;</td>
</tr>
<tr>
<td></td>
<td>• an individual’s express wishes about the future provision of health services to him or her;</td>
</tr>
<tr>
<td></td>
<td>• other personal information collected to provide, or in providing, a health service;</td>
</tr>
<tr>
<td></td>
<td>• other personal information collected in connection with the donation of human tissue; and</td>
</tr>
<tr>
<td></td>
<td>• genetic information that is or could be predictive of the health of an individual or their relatives or descendants.</td>
</tr>
<tr>
<td></td>
<td>For the purpose of this document, health information is included in the phrase personal information and a reference to ‘information’ in this document is a reference to both health and personal information.</td>
</tr>
<tr>
<td>All other terms</td>
<td>Definitions used in the <em>Privacy Act</em> are used in this document. Where a term does not appear in that Act, but in the <em>Health Records Act</em>, the corresponding definition applies.</td>
</tr>
</tbody>
</table>
CHAPTER 1 – INTRODUCTION

1.1 BACKGROUND – WHY WE HAVE A PRIVACY MANAGEMENT PLAN

WorkCover controls and maintains a variety of personal information. Under the Privacy Act, WorkCover is required to develop a Privacy Management Plan to detail how it will comply with the legislation.

With the introduction of the Health Records Act this Plan was reviewed by WorkCover to incorporate the requirements of this additional legislation into the Plan.

1.2 SCOPE – WHAT IS IN OUR PRIVACY MANAGEMENT PLAN

WorkCover’s Privacy Management Plan covers all personal information held by WorkCover.

WorkCover’s Privacy Management plan covers the following issues:

- policies necessary to ensure compliance by the agency with the Privacy Act and/or the Health Records Act;
- practices underpinning these policies;
- strategies to communicate these policies within the agency; and
- other matters that are considered relevant by WorkCover in relation to privacy and the protection of personal information and health information held by the agency.

1.3 STATUTORY REQUIREMENTS – WHAT LAWS IMPACT ON THE ACTIVITIES OF WORKCOVER

WorkCover works as a partner in the occupational health and safety, workers compensation and injury management systems set up under the requirements of the following:

- Occupational Health and Safety Act 2000
- Workers Compensation Act 1987
- Workplace Injury Management and Workers Compensation Act 1998
- Explosives Act 2003
- Workers Compensation (Bush Fire, Emergency and Rescue Services) Act 1987
- Workers Compensation (Dust Diseases) Act 1942
- Sporting Injuries Insurance Act 1978
- Rural Workers Accommodation Act 1969

1. WorkCover is also subject to any subsequent acts that are in force during the currency of this plan
In carrying out its role, WorkCover:

- provides information, education, advice and assistance to workplaces, enabling them to provide a safe, healthy and productive environment and prevent workplace injury and disease;
- promoting prompt, efficient and effective management of injuries to persons injured at work;
- ensuring efficient operation of workers compensation insurance arrangements;
- ensuring appropriate coordination of the administration of insurers under workers compensation legislation; and
- effectively managing investments that will be used to meet future claims.

1.4 LEGISLATION – WHAT LAWS IMPACT ON HOW WORKCOVER MANAGES INFORMATION

Legislation and its associated regulations, policies and standards, having statutory impact on the collection, storage, usage and disclosure of personal information at WorkCover includes:

New South Wales

1.4.1 State Records Act 1998
The State Records Act 1998 and State Records Regulation 2005 requires all public offices to make and keep full and accurate records regardless of their form. The State Records Authority of NSW issues records management standards under this Act.

The State Records Government Record Keeping Manual contains a current list of policies and standards. WorkCover has developed records keeping policy and practices in line with these requirements.

1.4.2 Privacy and Personal Information Protection Act 1998
This Act protects the rights of individuals as they relate to the collection, storage, usage and disclosure of personal information by New South Wales Government agencies.

1.4.3 Health Records and Information Privacy Act 2002
The purpose of this Act is to promote fair and responsible handling of health information. It aims to protect the privacy of an individual’s health information that is held in the public and private sectors, and enables individuals to gain access to their health information. It provides an accessible framework for the resolution of complaints regarding the handling of health information.

1.4.4 Freedom of Information Act 1989
The objectives of the FOI act are to extend the rights of the public to obtain access to information held by the Government and to ensure that records held by the government concerning the personal affairs of members of the public are not incomplete, incorrect, out of date or misleading.
1.4.5 **Evidence Act 1995**

Evidence legislation in Australia, as it relates to the work of record keeping professionals, is primarily concerned with the admissibility of documentary sources by a court of law.

To ensure WorkCover manages its electronic records that can be admissible in Court, WorkCover is required to implement a reliable electronic document management system to ensure WorkCover’s records are authentic and inviolate.

1.4.6 **Public Finance and Audit Act 1983**

The Public Finance and Audit Act 1983 requires all New South Wales Government agencies to keep proper accounts and records in relation to all of its operations.

The accounts and records of financial transactions of, or, relating to WorkCover, and the records of, or, relating to assets of or in the custody of WorkCover or the liabilities of WorkCover, shall be inspected and audited by the Auditor-General.

1.4.7 **Crimes Act 1900**

This Act provides that any person who steals, unlawfully and maliciously cancels, obliterates, injures, or destroys any record or document of any Court or relating to the business of any office or employment under Her Majesty, and being in any public office, shall be liable to imprisonment for seven years.

1.4.8 **Electronic Transactions Act 2000**

This Act provides a regulatory framework that recognises the importance of the information economy to the economic and social prosperity of Australia, facilitates the use of electronic transactions, promotes business and community confidence in the use of electronic transactions, and enables business and the community to use electronic communications in their dealings with government.

1.4.9 **Workplace Surveillance Act 2005**

This Act prohibits the surveillance by employers of their employees at work except where employees have been given notice or where the employer has a covert surveillance authority. It also restricts and regulates the blocking of emails and internet access of employees at work. It extends beyond the workplace to any place where an employee is working.

1.4.10 **Workplace Injury Management and Workers Compensation Act 1998**

This Act provides for the effective management of work-related injuries and injury compensation for workers in respect of such injuries. It prohibits disclosure of information obtained in connection with the administration or execution of that Act, except in certain prescribed circumstances. Personal information may be provided or gathered under this Act. The Act also allows WorkCover to compel the production of information, which may include personal information.
1.4.11 Workers Compensation Act 1987
This Act provides for the compensation and rehabilitation of workers in respect of work related injuries. Personal information may be provided or gathered under this Act. The Act also allows WorkCover to compel the production of information, which may include personal information.

1.4.12 Explosives Act 2003
This Act provides for the regulation and control of the handling of explosives and explosive precursors and certain other dangerous goods. It authorises the disclosure of information outside New South Wales in certain circumstances.

1.4.13 Occupational Health and Safety Act 2000
The purpose of this Act is to secure the health, safety and welfare of people at work. Personal information may be provided or gathered under this Act. Under this Act, WorkCover inspectors have power to compel the production of information, which may include personal information.

Commonwealth
1.4.9 Privacy Act 1988
This Act protects the rights of individuals as it relates to the collection, storage, usage and disclosure of personal information by some private sector organisations and Commonwealth and ACT Government agencies.

1.4.10 Electronic Transaction Act 1999
This Act provides a regulatory framework that recognises the importance of the information economy to the economic and social prosperity of Australia, facilitates the use of electronic transactions, promotes business and community confidence in the use of electronic transactions, and enables business and the community to use electronic communications in their dealings with government.

1.4.11 Freedom of Information Act 1982
The object of this Act is to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth\(^2\).

1.4.12 Mutual Recognition Act 1992
The purpose of the *Mutual Recognition Act 1992* is to promote the goal of freedom of movement of goods and service providers in a national market in Australia. It permits disclosure of information to interstate registration authorities where information is required in connection with a notice lodged by a person seeking registration or actual or possible disciplinary action.

---

1.5 PRIVACY CODES OF PRACTICE – PUBLIC INTEREST DIRECTIONS

A Privacy Code of Practice under the Privacy and Personal Information Protection Act 1998 is a statement of how an agency proposes to depart from the Information Protection Principles or the public register provisions of the Privacy Act.

It is not, like a normal code of practice or a code of conduct, a statement of the ethical standards WorkCover follows to protect privacy. Nor is it meant to be a comprehensive guide to WorkCover’s information management practices.

The Office of the Privacy Commissioner prepares or approves Privacy Codes of Practice. WorkCover then can assess whether or not it should adopt them.

WorkCover has adopted the Privacy Code of Practice for the Workforce Profile that has been prepared by the Office of the Privacy Commissioner.

Public Interest Directions

In addition, the Privacy Commissioner can develop Public Interest Directions, which apply temporarily until the Attorney General makes an appropriate privacy code of practice.

At the time of writing, the following directions applied to WorkCover:

- Direction on disclosures of information by New South Wales Public Sector Agencies for research purposes;
- Direction on information transfers between New South Wales Public Sector Agencies; and
- Direction on processing of personal information by New South Wales Public Sector Agencies in relation to their investigative functions.

1.6 WORKCOVER EXTERNAL DATA RELEASE POLICY

During the course of compiling data, some rates of incidence or claim information may be so small that it’s possible to identify or draw conclusion regarding individual(s). In these instances WorkCover will determine that these figures are to be reported as N.P (Not Published) to protect the identity of those individuals. This is carried out in line with the requirements of the Privacy Act.
CHAPTER 2 – PRIVACY MANAGEMENT POLICY

2.1 POLICY – OUR COMMITMENT TO INFORMATION PRIVACY

Personal information collected by WorkCover will be managed in accordance with all relevant legislation.

All personal information will be managed so as to meet the requirements of the information protection principles contained in the Privacy Act and Health Records Act. A summary of the principles is set out in the following table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection</td>
<td>1. <strong>Lawful</strong> – An agency must not collect personal information unless it is collected for a lawful purpose directly related to the agency’s activities and the collection is reasonably necessary for that purpose. (section 8)</td>
<td>1. <strong>Lawful</strong> – An organisation must not collect health information unless it is collected for a lawful purpose directly related to the agency’s activities and the collection is reasonably necessary for that purpose. (cl 1, Sch 1)</td>
</tr>
<tr>
<td></td>
<td>2. <strong>Direct</strong> – personal information must be collected directly from the individual, unless that person authorises collection from someone else. Parents and guardians can provide personal information for minors. (section 9)</td>
<td>2. <strong>Direct</strong> – health information must be collected directly from the person concerned, unless it is unreasonable or impracticable to do so. (cl 3, Sch 1)</td>
</tr>
<tr>
<td></td>
<td>3. <strong>Open</strong> – an agency must ensure that individual is informed that the personal information is being collected, the purposes for which it is being collected, the intended recipients of the information, whether the supply of the information is required by law or voluntary, the existence of any right to access or correct the information and details of the agency collecting and storing it. (section 10)</td>
<td>3. <strong>Open</strong> – an organisation must take reasonable steps to ensure person is aware of the contact details of the organization, the fact that they can request access, the purposes for which the health information is being collected, what will be done with it and who might see it. The agency should also inform the person how they can view and correct their health information, any legal requirements to provide the information and any consequences if they do not provide their information. If health information is collected about a person from someone else, reasonable steps must be taken to ensure that the person has been notified as above. There are some exceptions – such as where the individual has consented, where the organisation is lawfully authorised or required not to comply, or where compliance might detrimentally affect the investigative functions of an agency. (cl 4, Sch 1).</td>
</tr>
<tr>
<td>4. Relevant – an agency must take reasonable steps (depending on the purpose for collecting the information) to ensure that personal information is relevant for the purpose it was collected, accurate, up-to-date, and not excessive. The collection should not unreasonably intrude into the individual’s personal affairs. (section 11)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Relevant – an organisation must take reasonable steps (depending on the purpose for collecting the information) to ensure that the health information is relevant, not excessive, accurate, up-to-date and complete. The collection should not unreasonably intrude into the individual’s personal affairs. (cl 2, Sch 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Retention and security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Secure – an agency that holds personal information must ensure it is stored securely and not kept any longer than necessary, and disposed of appropriately. It should be protected by reasonable security safeguards from unauthorised access, use or disclosure. (section 12)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Secure – health information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected by reasonable security safeguards from unauthorised access, use or disclosure. (cl 5, Sch 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Transparent – an agency must take reasonable steps to enable a person to work out whether the agency holds personal information, whether it holds personal information about that person and if it does hold personal information about that person, the nature of the information, why they are storing it and what rights an individual has to access it. (section 13)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Transparent – an organisation must provide enough detail to an individual about what health information on that person they are storing, why they are storing it and what rights an individual has to access it. (cl 6, Sch 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Accessible – the agency must allow an individual, on request, to access their personal information without unreasonable delay and expense. (section 14)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. Accessible – an organisation must allow people access to their health information, on request, without unreasonable delay or expense. (cl 7, Sch 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Correct – the agency must allow an individual, on request, to update, correct or amend their personal information to ensure it is accurate, up-to-date, complete and not misleading. It must also notify recipients of that amendment, if reasonably practicable. If the agency is not prepared to amend the personal information, it must take reasonable steps to attach to the information a statement provided by the individual of the amendment sought. (section 15)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Correct – the organisation must allow an individual, on request, to update, correct or amend their health information to ensure it is accurate, up-to-date, complete and not misleading. It must also notify recipients of that amendment, if reasonably practicable. If the agency is not prepared to amend the personal information, it must take reasonable steps to attach to the information a statement provided by the individual of the amendment sought. (cl 8, Sch 1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Use</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Accurate – agencies must take reasonable steps to ensure that personal information is accurate, relevant, up-to-date, complete and not misleading before using it. (section 16)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Accurate – an organisation must take reasonable steps to ensure that health information is accurate, relevant, up-to-date, complete and not misleading before using it. (cl 9, Sch 1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Information Protection Principles

<table>
<thead>
<tr>
<th>Privacy and Personal Information Protection Act 1998</th>
<th>Health Records and Information Privacy Act 2002</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10. Limited</strong> – agencies must not use personal information for a purpose other than that for which it was collected, unless for a directly related purpose, or for a purpose to which the individual has given consent or in order to prevent or lessen a serious and imminent threat to any person’s life or health. (section 17)</td>
<td><strong>10. Limited</strong> – an organisation must not use health information for a purpose other than the purpose for which it was collected, unless it is for directly related purpose that the person would reasonably expect, or the person has given consent or it falls within another authorised secondary purpose (including where there is a serious threat to health or welfare; for the management of a health service, for training, research, to find a missing person, investigation of suspected unlawful activity, unsatisfactory professional conduct or breach of discipline, law enforcement, or to exercise complaint handing or investigation functions. (cl 10, Sch 1)</td>
</tr>
</tbody>
</table>
| **Disclosure** | **11. Restricted** – the agency must not disclose personal information unless:  
  - if it is for a related purpose and it doesn’t think that the individual would object  
  - the individual is reasonably likely to have been aware that information is usually disclosed to that person or body  
  - in order to prevent or lessen a serious and imminent threat to any person’s life or health. (section 18)  
**11. Limited** – an organisation must not disclose health information for a purpose other than the purpose for which it was collected unless it is for a directly related purpose that the person would expect, or the person has given consent, or it falls within another authorised secondary purposes (including where there is a serious threat to health or welfare; for the management of a health service, for training, research or compassionate reasons, to find a missing person, for investigation of suspected unlawful activity, unsatisfactory professional conduct or breach of discipline, law enforcement, or to exercise complaint handing or investigation functions. (cl 11, Sch 1) |
| **12. Special Limits on Disclosure** – the agency must not disclose an individual’s sensitive personal information, for example information about ethnic or racial origin, political opinions, religious or philosophical beliefs, health or sexual activities or trade union membership unless the disclosure is necessary to prevent a serious and imminent threat to any person’s life or health. (section 19) | **12. Not identified** – individuals should only be identified by using unique identifiers if it is reasonably necessary to carry out the agency’s functions efficiently. (cl 12, Sch 1) |
| **Identifiers & Anonymity** | |

---

10
<table>
<thead>
<tr>
<th>Transferals &amp; Linkage</th>
<th>13. Anonymous – people must be given the option of receiving services from an agency anonymously where this is lawful and practicable. (cl 13, Sch 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>13.</strong> Following the making of a privacy code of practice, personal information must not be disclosed to a person or body outside New South Wales or to a Commonwealth agency unless a relevant privacy law applies and is in force or disclosure is permitted under a privacy code of practice (section 19)</td>
<td></td>
</tr>
<tr>
<td>14. Controlled – health information must only be transferred outside New South Wales if an organisation reasonably believes that the recipient is subject to laws or obligations substantially similar to the Health Privacy Principles, or consent has been given, or transfer is under a contract between an organisation and the individual, or transfer will benefit the individual, it is impracticable to obtain the individual’s consent but individual would be likely to consent; or an organisation reasonably believes transfer is necessary to lessen or prevent serious or imminent threat to life, health or safety of a person or a serious threat to public health or safety; or an organisation has taken reasonable steps to ensure information transferred will not be held, used or disclosed inconsistently with Health Privacy Principles, or transfer is handled inconsistently with the Health Act or transfer is permitted or required by law(cl 14, Sch 1)</td>
<td></td>
</tr>
<tr>
<td>15. Authorised – an organisation must not include health information in any system that links health records across more than one organisation unless the person expressly consents. Health information or the disclosure of their identifier for the purpose of the health records linkage system, should only be included if the person has given express consent (cl 15, Sch 1)</td>
<td></td>
</tr>
</tbody>
</table>
2.2 COMPLIANCE – HOW WE MEET THE INFORMATION PROTECTION PRINCIPLES

Collection

2.2.1 Lawful

All information collection will be carried out under the obligations imposed on WorkCover by its governing legislation and administrative requirements.

2.2.2 Direct

Where information is collected directly from the individual, a statement will appear on the collection instrument to ensure that WorkCover complies with this principle.

2.2.3 Open

Where information is being collected, a statement will appear on the collection instrument to ensure that WorkCover complies with this principle.

2.2.4 Relevant

In the process of collecting personal information WorkCover will ensure that the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete. WorkCover will ensure the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

Storage

2.2.5 Secure

WorkCover will ensure that information is:

• kept for no longer than is necessary for the purposes for which the information may lawfully be used through the use of an approved sentencing schedule, disposal authority and storage standard;

• disposed of securely and in accordance with any requirements for the retention and disposal of personal information;

• protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse through the use of secure information systems and operational policies and procedures; and

• only provided to a person in connection with the provision of a service to WorkCover, and that everything reasonably within the power of WorkCover is done to prevent unauthorised use or disclosure of the information.

2.2.6 Transparent

WorkCover will take such steps that are, in the circumstances, reasonable to enable any person to ascertain:

• whether WorkCover holds personal information;

• whether WorkCover holds personal information relating to that person; and

• if WorkCover holds personal information relating to that person, the nature of that information, the main purposes for which the information is used, and that person’s entitlement to gain access to that information.
2.2.7 Accessible

WorkCover, at the request of the individual to whom the personal information relates and without excessive delay or expense, will provide the individual with access to the information.

2.2.8 Correct

WorkCover, at the request of the individual to whom the information relates, will make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information is accurate, relevant, up to date, complete, and not misleading. Where the information has been collected via Scheme agents, the agent will be requested to amend the information.

If it is not considered appropriate for WorkCover to amend personal information in accordance with a request by the individual to whom the information relates, WorkCover will, if requested by the individual concerned, take reasonable steps to attach to the information any statement provided by that individual of the amendment sought so that this information can be viewed alongside the original information.

In the amendment of personal information, WorkCover permits the individual to whom the information relates, if it is reasonably practicable, to have recipients of that information notified of the amendments made by WorkCover.

2.2.9 Accurate

WorkCover will not use personal information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

2.2.10 Limited

WorkCover will not use personal information for a purpose other than that for which it was collected unless the:

- individual to whom the information relates has consented to the use of the information for that other purpose; or
- other purpose for which the information is used is directly related to the purpose for which the information was collected;
- use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person;
- use of the information is reasonably necessary for staff training, or research and analysis if it is the public interest;
- other uses consistent with the conditions outlined in HPP 10;
- WorkCover believes on reasonable grounds that the disclosure is necessary to assist in an investigation that may lead to prosecution;
- or other reasons consistent with the conditions outlined in HPP 11.
Disclosure

2.2.11 Restricted

WorkCover will not disclose personal information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless:

- the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure; or
- the individual concerned is reasonably likely to have been aware, or has been made aware that information of that kind is usually disclosed to that other person or body; or
- WorkCover believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; or
- WorkCover believes on reasonable grounds that the disclosure is necessary to assist in an investigation that may lead to prosecution.

Personal information is disclosed in accordance with the above criteria to a person or body that is a public sector agency or an organisation that is authorised by legislation administered by WorkCover. That agency or organisation shall not use or disclose the information provided by WorkCover for a purpose other than the purpose for which the information was given to it.

2.2.12 Safeguarded

WorkCover will not disclose personal information relating to an individual’s ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

2.2.13 Not identified

Individuals are only identified by using unique identifiers if it is reasonably necessary to do so in order to carry out the agency’s functions efficiently.

Identifiers and Anonymity

2.2.14 Anonymous

Where lawful and practical, individuals are given the opportunity to not identify themselves when entering into transactions with or receiving health services within the Workers Compensation Scheme.
Transferrals and linkage

2.2.15 Controlled

WorkCover shall not disclose personal information to any person or body who is in a jurisdiction outside New South Wales unless the disclosure complies with the requirements outlined above at 2.11 (Restricted). However, this may not apply if WorkCover is otherwise authorised by law to disclose the personal information outside New South Wales or to a Commonwealth agency. Examples of other legislation which may authorise WorkCover to disclose personal information outside New South Wales or to a Commonwealth agency include:

- the Mutual Recognition Act 1992 (Cth)
- the Explosives Act 2003 (NSW).

If a privacy code of practice is made by the Privacy Commissioner relating to the disclosure of personal information by public sector agencies to persons or bodies outside New South Wales and to Commonwealth agencies, other restrictions on cross-border disclosure of personal information will apply.

WorkCover does not transfer health information outside New South Wales unless it is in accordance with the conditions set out in HPP14.

2.2.16 Authorised

WorkCover endeavours to gain consent before transferring claims data and health records across more than one organisation, and only discloses or uses identifiable health information to other organisations with consent.

2.3 PUBLIC REGISTER – HOW WE COMPLY WITH THE PUBLIC REGISTER PROVISIONS

2.3.1 Disclosure of personal information contained in public registers

A public register is a register of information that is required by law to be made publicly available.

WorkCover will not disclose any personal information kept in a public register unless WorkCover is satisfied that it is to be used for a purpose relating to the purpose of the register or the Act under which the register is kept.

WorkCover may require any person who applies to inspect personal information contained in a public register held by WorkCover to give particulars, in the form of a statutory declaration, as to the intended use of any information obtained from the inspection.

WorkCover collects, accesses, and has custodianship of records relating to the following publicly available information and public registers:

- WorkCover Board Minutes;
- Return to Work Coordinator Trainers;
- Rehabilitation Providers;
- Injury Management Consultants;
- First Aid Provider;
- Approved Medical Specialists;
- Health Care providers – physiotherapists, chiropractors, osteopaths, exercise physiologists and remedial massage therapists
- Permanent Impairment Assessors;
- Public Assessors;
- OHS Construction Induction Accredited Trainers;
- OHS Consultation Accredited Trainers;
- Operator Certification Assessors; and
- Clothing Factory Register.

2.3.2 Restricted registers
WorkCover currently has no restricted registers.

2.3.3 Suppression of personal information
A person about whom personal information is contained (or proposed to be contained) in a public register may request WorkCover to have the information:
• removed from, or not placed on, the register as publicly available; and
• not disclosed to the public.

If WorkCover is satisfied that the safety or well-being of any person would be affected by not suppressing the personal information as requested, WorkCover shall suppress the information in accordance with the request unless WorkCover is of the opinion that the public interest in maintaining public access to the information outweighs any individual interest in suppressing the information.

WorkCover reserves the right for any information that is removed from, or not placed on, a public register to be kept on the register for other purposes in accordance with the provisions of its governing legislation.

2.4 CONTINUOUS IMPROVEMENT – HOW WE IMPROVE WHAT WE DO

Section 33 of the Privacy Act relates to the preparation and implementation of privacy management plans. WorkCover, as a public sector agency, was required to prepare and implement a privacy management plan within 12 months of the commencement of this section. Section 33 commenced on 1 July 1999.

The first plan was developed in 2000, reviewed in 2006 and 2008.

WorkCover will review its privacy management plan every three years, which will include review of:
• policies that underpin privacy management practice and ensure compliance by the agency with the requirements of this Act;
• practices and procedures to support the policies, including internal review procedures;
• the dissemination of those policies and practices to persons within the agency;
• strategies for the following three years to enhance personal information management; and
• such other matters as are considered relevant by WorkCover in relation to privacy and the protection of personal information held by the agency.

At the conclusion of each review, WorkCover will provide a copy of its Privacy Management Plan to the Privacy Commissioner as soon as practicable after it is amended.

2.5 REPORTING – HOW WE LET PEOPLE KNOW ABOUT INFORMATION MANAGEMENT

WorkCover’s Annual Report will:

• include a statement of the action taken in compliance with the requirements of the Privacy Act;
• include statistical details of any review conducted under Part 5 of the Privacy Act; and
• be available on the WorkCover website.

A copy of the Privacy Management Plan will be available on WorkCover’s website.
3.1 INFORMATION – WHAT SIGNIFICANT PERSONAL INFORMATION IS HELD BY 
WORKCOVER

In the course of carrying out its functions WorkCover collects the following personal information:

3.1.1 Corporate Services Division

3.1.1.1 Business Risk Management and Site Services Branch

Personal information such as emergency contacts, leave applications, after hours contact, drivers licence details, CCTV footage and photographs of individuals.

3.1.1.2 Communications Group

Various mailing lists relating to seminar and event attendance, publication distribution lists, electronic news subscriptions and customer assistance records.

3.1.1.3 Finance Branch

Names and addresses of suppliers, including bank details.

Names and addresses of customers which may include financial details.

Personal and financial details of persons paid under the Uninsured Liability and Indemnity Scheme or the Bushfire, Emergency and Rescue Services Scheme.

3.1.1.4 Human Resources Branch

Human resource information, such as job applications, phone numbers including emergency contact phone numbers, work history, skills and qualification, grading classification, salary, leave records.

Includes performance management details, workers compensation details, medical reports, dispute resolution and complaint data.

3.1.1.5 Information Technology Service Branch

Human resource information, such as job applications, phone numbers, work history, skills and qualification, grading classification, salary, leave records and medical certificates.

Emergency details for contact during disaster recovery or out-of-hours callout.

Records of investigation into alleged inappropriate usage of WorkCover assets. These may include emails or electronic files of a non-work related nature and which may contain personal details.
3.1.6 Legal Group

Litigation and advice files.

Human resource information such as contact details and leave applications.

Personal information and possibly health information of family members of deceased persons for the WorkCover bereavement service.

3.1.2 Workers Compensation Division

3.1.2.1 Agent Operations Group

Obtains information about claims and policies as part of its role in monitoring the performance of individual Scheme agents and the Scheme in general.

Access to claims and policies information within the WorkCover scheme, such as medical, legal and financial information. This information is held within the WorkCover Corporate Data Repository.

3.1.2.2 Provider and Injury Management Services Group

Information relating to injured workers, including personal details such as dependents home address, health details, income and employment details including tax file numbers.

Information regarding complainants, which may include name, address and phone number.

Information relating to injured persons covered under the Uninsured Liability and Indemnity Scheme or the Bushfire, Emergency and Rescue Services Scheme, including personal details such as dependents home address, health details, income and employment details including tax file numbers.

Information relating to work trials, home modification requests, treatment providers, return to work surveys, treatment providers and service providers (contact details, address, email and telephone numbers).

3.1.2.3 Regulatory and Financial Services Group

Self & Specialised Insurers: A List of Licensed Entities is kept with the following information – postal and email addresses, phone and fax numbers, CV’s of employers within the licensed entities which includes date of birth, home address and academic qualifications.

Workers Compensation Insurance Fund: Westpac Corporate on line system, which includes names, date of birth, addresses, drivers licence details, passports and birth certificates.

WorkCover Status Rulings Branch: Names, phone numbers, postal and email addresses, information on the business, ABN’s and Workers Compensation Policy details.
**Fraud Branch:** Names, phone numbers, wage records, medical records, claims files, drivers license details, bank account numbers and transaction details.

### 3.1.2.4 Premiums Group

Employer business information and limited personal information of workers with regard to premium-related matters and commutation applications.

### 3.1.2.5 Business Analysis and Strategy Group

Information collected from the WorkCover Corporate Data Repository and other WorkCover corporate databases.

Expressions of Interest for WorkCover’s scholarship program and for merit/experienced based participation in working/focus/reference groups.

The information collected may include names, addresses, claim details including claimant characteristics, injury and cost, contact details personal resumes or other professional background details and qualifications.

### 3.1.3 Occupational Health & Safety Division

#### 3.1.3.1 Strategic Specialist Services Group

**Major Hazard Facilities:** Information collected relates to companies or agencies, including contact details for employees of these companies or agencies eg – work contact details.

**Working Environment Team/Unit:** Various information held via field investigation assistance. (All collected as per inspector protocols and under inspector Authorities).

**Response Team:** Complainant and investigation details - such as involved parties, injured persons, deceased persons and witnesses.

**Manual Handling Summit Response Program:** Information collected via the Smart Move website when people order posters and register to use discussion boards. Details are also collected when manual handling events are attended.

**Asbestos and Demolition:** Personal information of licence holders.

**Engineering Team:** inspector notes contain personal information and details of injuries.
3.1.3.2 Operational and Tactical Support Group

Information collected for WorkCover accredited Assessors and Trainers such as names (including company names), postal and email addresses, home, work and mobile phone numbers, payment details (for payment of fees and purchase of Notice of Satisfactory Assessment books), evidence of identity – certified copies of drivers licence, passport, Medicare Card, birth certificate or Citizenship papers, conviction records (information for criminal record checks), employment details, references (written and contact numbers) and qualifications, signed declarations.

Names and addresses collected for assessment papers and application forms for national certificates of competency for construction induction training or assessments for explosive power tools or formwork.

3.1.3.3 Business Assistance Branch

Mailing lists relating to seminar and workshop attendance.

3.1.3.4 Industry Relationships Group

Complaints and investigations information, which may include photographs, statements, incident and injury.

Human resource information such as medical certificates, training records, photographs belonging to parties involved in complaint, incident and injury investigations and held in official files.

Workers compensation claims information including medical certificates, return to work details.

Database of participants in workshops and seminars.

Legal records.

3.1.3.5 Laboratory and Testing Services – TestSafe

Health data collected as part of testing services, which include blood and urine samples and given the names, date of birth and address details.

3.1.4 Investment Division

Personal information collected relating to the Workers Compensation Insurance Fund Investment Board members – contact details and pecuniary interests, addresses and contact details. Resumes of candidates provided by recruitment consultancies and contact information of current staff.

3.1.5 Internal Audit Unit

Personal information may be collected for the use of investigative purposes only.
3.1.6 Office of Chief Executive

Personal information that might arise as a result of the secretariat services provided to the WorkCover Executive, the WorkCover Board and the Workers Compensation and Workplace Occupational Health and Safety Council.

Personal information collected through the WorkCover’s Compliments and Complaints Handling Policy and Procedures.

3.1.6.1 NSW Sporting Injuries Committee

Information relating to injured sportspersons covered under the Sporting Injuries Insurance Act 1978, including personal details such as names, home addresses and contact details, health details and medical reports, income (employment details including tax file numbers), asset registers and information about dependents.

Mailing lists including organisation names, office bearer names and mailing and emailing addresses.

Personal details of office bearers for sporting organisations.


Personal and some financial details of Committee members.

3.1.7 Strategy and Policy Division

3.1.7.1 Executive and Ministerial Services Unit

Name, addresses and other personal details as provided by persons that correspond with the Chief Executive Officer or Minister.

Personal information contained in the processing of Freedom of Information and Privacy requests.

3.1.7.2 Knowledge Management

Injured workers details, including names address, injury, rehabilitation and compensation, medical information, wage information.

Employer workers compensation policy and claim details.

Human resource information such as staff medical certificates.

Resumes containing personal information for contractors.

Emergency details for contacting staff for business continuity processes.

Information on deceased persons via the National Coronial Inquest System.
3.1.7.3 Policy, Regulation and Planning Branch

Personal details relating to:

- contract, grant and research activities;
- national committees;
- submissions relating to regulatory developments; and
- register of attendees at public information sessions.

3.1.7.4 Strategic Projects Unit

Information collected relating to notified workplace fatalities for the Australian Safety and Compensation Council and Workers Compensation and Workplace Occupational Health & Safety Council.

3.2 HOW WORKCOVER MANAGES PERSONAL INFORMATION

All records held by WorkCover are managed in accordance with WorkCover’s Record keeping policies. These policies cover all types of WorkCover records in any format including documents (paper and electronic), data in business information systems, verbal decisions and objects (eg photographs, maps, evidence and samples).

3.3 HOW WORKCOVER MANAGES ACCESS TO AND AMENDMENT OF PERSONAL INFORMATION

Persons wishing to access or amend their personal information must lodge their application in writing. A $30 fee applies to applications for access. Applications should be sent to:

Privacy Contact Officer
WorkCover NSW
Locked Bag 2906
LISAROW NSW 2252

A 50 per cent reduction in fees and charges applies if an applicant:

- holds a Pensioner Concession Card or Health Care Card issued by the Commonwealth;
- has a weekly income less than the maximum weekly income allowable under the Commonwealth Social Security Act 1947, to holders of such a card;
- holds a War Widow Concession Card;
- is under the age of 18 years; or
- submits an application relating to information that is in the public interest to make available.

One reduction in fees only may be given in respect each application. For example, a young person under the age of 18 years but in receipt of a pensioner health benefit card could not obtain both a 50 per cent reduction for financial hardship and a further 50 per cent reduction for being under the age of 18 years in relation to the one application.

Applications are not required to be on a specific form, but must state that the information is sought under the Privacy Act or Health Records Act.
Where a person seeks access to personal information, their identity should be verified. This requires that the person provide documentary evidence of proof of identity. The amount of identification required will vary according to the nature of the document(s) requested and the sensitivity of the personal information recorded on the document.

The officer who has been identified to act as the Privacy Contact Officer will process applications. Applications will be recorded according to record keeping policies.

Should a privacy application be made on personal information in a protected document, the applicant may be given an extract of the information containing only the information that is deemed by WorkCover to be personal information of the applicant.

A response to the application will be made within 21 days.

The Privacy Officer can make arrangements, where practicable, for access to WorkCover records containing personal and private information at a WorkCover location other than the head office.

The Privacy Contact Officer will develop, maintain and manage systems to allow people to obtain access to documents and to seek to amend documents about their personal affairs.

### 3.4 HOW WORKCOVER MANAGES COMPLAINTS ABOUT ITS CONDUCT UNDER THE PRIVACY AND HEALTH RECORDS ACTS

A person (the complainant) who is aggrieved by the conduct of WorkCover is entitled to a review of that conduct. They must make their complaint within 6 months of becoming aware of the conduct.

Conduct that can be reviewed is:

- the contravention of an information protection principle that applies to WorkCover;
- the contravention of a privacy code of practice, if any, that applies to WorkCover; and
- the disclosure by WorkCover of personal information kept in a public register.

Complainants must lodge their complaints in writing. WorkCover will use the Internal Review Application Form, found at www.lawlink.nsw.gov.au/lawlink/privacynsw until such time as it has developed a form for this purpose.

Applications are not required to be on this form, but must state that they seek an internal review under the Privacy Act or Health Records Act.

The officer who has been identified to act as the Privacy Contact Officer will process applications unless they have been involved in the complaint(s) relating to conduct. In that case, the Privacy Contact Officer will appoint a Reviewing Officer to conduct the review.

Complaints will be recorded according to record keeping policies.

The Privacy Contact Officer or Reviewing Officer will be required to follow the Privacy Complaint/Internal Review Checklist developed by Privacy NSW.

Within seven days of receipt of the complaint, the Privacy Commissioner must be notified of a complaint and briefed on its progress.
The review is to be completed within 60 days of lodgement of the complaint. In the response to the complainant, the complainant must be advised of their rights to appeal the decision.

The Privacy Commission must be advised of the outcome of the internal review within 7 days of completion of the review.

The Privacy Contact Officer will develop, maintain and manage systems to allow people to lodge internal reviews.

3.5 **HOW WORKCOVER WILL DISSEMINATE PRIVACY POLICIES AND RELATED INFORMATION**

Policies, procedures and related information will be made available to all WorkCover personnel via the WorkCover Intranet. It is a WorkCover policy that all WorkCover personnel have access to the WorkCover Intranet. The Intranet site is updated with current information as and when required.

The Privacy Contact Officer has responsibility for all content relating to the *Privacy Act* and *Health Records Act* on the WorkCover Internet and Intranet sites.

Staff members will be provided with training on their obligations under the *Privacy* and *Health Records Acts* during WorkCover’s induction courses.

A copy of the Privacy Management Plan will be available on WorkCover’s Internet and Intranet sites.

A statement of the action taken by WorkCover in complying with these Acts, including statistical data on internal reviews, will be included in WorkCover’s Annual Report.