

# Practice Code for the Use of Personal Health Information

# CONTENTS

<b>Introduction .....</b>	<b>3</b>
<b>1 The Principal Investigator .....</b>	<b>5</b>
<b>2 Security of Personnel .....</b>	<b>5</b>
Authorised Persons.....	5
Obligations.....	6
<b>3 Use and Disclosure of Personal Health Information .....</b>	<b>6</b>
Restrictions on Use and Disclosure .....	6
Contact with Individuals.....	7
Obligations.....	7
<b>4 Information Security .....</b>	<b>7</b>
Electronic Records .....	8
Paper Records.....	9
Containment of Breaches.....	10
Obligations.....	10
<b>5 Information Retention and Disposal.....</b>	<b>11</b>
Retention.....	11
Disposal.....	11
Obligations:.....	12
<b>6 Reporting and Monitoring .....</b>	<b>13</b>
Monitoring Reports .....	13
Modifications to Approved Projects.....	13
Retention and Destruction of Information.....	13
Breaches, Complaints and Adverse Events .....	14
Obligations:.....	14
<b>7 Publication .....</b>	<b>14</b>
Obligations:.....	15
<b>Acknowledgments.....</b>	<b>16</b>
<b>Appendix 1 .....</b>	<b>17</b>

## Introduction

The Department of Health WA (DOHWA) maintains health data collections on behalf of the people of Western Australia. The data collections contain the personal health information of individuals and are used to monitor the health of Western Australians and support the effective delivery of health services.

The information is used for the planning, management and monitoring of health services, and for epidemiological analysis and health related research. It is also used to meet funding and performance reporting obligations.

*The Department of Health WA Practice Code For the Use of Personal Health Information* (Practice Code) contains the guidelines that must be followed in the design and conduct of all projects using personal health information provided by the Department of Health. All applications for data for the purposes of funding, management, planning, monitoring, improvement or evaluation of health services, for training, research, compilation or analysis of statistics in the public interest must comply with this Practice Code. It outlines the matters that must be addressed to ensure the security and confidentiality of the information. It sets out the obligations that are imposed on all users of information provided by the Department of Health. The Practice Code represents the minimum standard of practice. Data Managers may require additional standards for some health data collections.

Information about the data collections, the DOHWA application procedures and the requirements for Human Research Ethics Committee approval can be found at <http://www.health.wa.gov.au/healthdata/hrec/index.cfm>

### Application of the Practice Code

This Practice Code applies to all requests to use personal health information in data collections held by the DOHWA. It applies to all applicants including those within the Department of Health, those from other State and Commonwealth agencies and all other external users.

### Personal Health Information

Personal health information includes information or opinions that relate to the health of a person where the identity of a person is apparent or can reasonably be ascertained from the information.

An individual is identifiable if the information contains the name of an individual, or other identifying items such as birth date, address or geocoding. An individual will be identifiable if the information contains a unique personal identifier and the holder of the information also has the master list linking the identifiers to individuals. An individual may be identifiable because of the number of different pieces of information known about a particular individual. An individual will also be identifiable where the person holding the information can link it to other information that is identified. It may also be possible to ascertain the identity of individuals from aggregated data where there are very few individuals in a particular category. Identifiability is dependent on the amount of information held and also on the skills and technology of the holder. The individual identified may be a patient or a health care provider. In every case a judgement must be made as to whether the identity of an individual can reasonably be ascertained by the holder of the information.

## Structure of the Practice Code

**Section 1, The Principal Investigator,** requires the nomination of a principal investigator who will take responsibility for the management of the project.

**Section 2, Security of Personnel,** establishes a process for ensuring that everyone who works on the project understands their obligations to maintain confidentiality and protect the security of the information.

**Section 3, Use and disclosure of Personal Health Information,** outlines the restrictions on the use and disclosure of the information to ensure that confidentiality and privacy are maintained.

**Section 4, Information Security,** describes the matters that must be addressed in a security plan to protect the information.

**Section 5, Information Retention and Disposal,** specifies the matters that must be addressed in a Retention and Disposal plan for the data on completion of the project.

**Section 6, Reporting and Monitoring,** outlines the reporting obligation that must be met.

**Section 7, Publication,** describes the expectations and obligations in the publication of research results.

# 1 The Principal Investigator

- 1.1 Every application for access to personal health information held in a data collection by the Department of Health must nominate a Principal Investigator who is responsible for compliance with this Practice Code and the protocol and conditions approved by the Department of Health WA Human Research Ethics Committee (DOHWA HREC) and the DOHWA. The Principal Investigator must be the person who has the immediate responsibility for the management of the project. This is not necessarily the same person as the chief investigator named on any funding grants. Where the application is made for a student project the Principal Investigator should be the student's supervisor. The Principal Investigator must be sufficiently senior to undertake the obligations outlined in this Practice Code and is required to undertake personal responsibility for the management of the project and the reporting requirements.

# 2 Security of Personnel

- 2.1 All personnel who have access to personal health information provided by DOHWA are bound by duties of confidentiality and legal obligations to protect the privacy of the individuals whose information is being used. The following guidelines must be followed to ensure that all personnel are aware of and comply with those duties and obligations.

## Authorised Persons

- 2.2 All project personnel with access to personal health information provided by DOHWA must sign a Confidentiality Agreement. Project personnel who are external to the Public Service must sign a *Confidentiality Agreement for Researchers* relating to each relevant project or application and must comply with that agreement. Public Service applicants must sign the appropriate internal Confidentiality Agreement.
- 2.3 All project personnel must be familiar with this Practice Code and the security protocol approved for the particular project or application.
- 2.4 An authorised person is a person who has signed a Confidentiality Agreement relating to the relevant project or application.
- 2.5 Only people authorised to work on the particular project may have access to personal health information provided for that project.
- 2.6 All system support staff who have access to personal health information through their role in maintaining information systems and data base administration must be bound by a confidentiality agreement with their employer that has been approved by DOHWA HREC.
- 2.7 Notification must be given of any proposed change in the project personnel who have access to personal health information released by the DOHWA. Notification should be sent to the DOHWA Data Services Office in the Department of Health who will forward the notice to the relevant Data Managers and DOHWA HREC.

## Obligations

### 2.8 The Principal Investigator is responsible for:

- Careful selection of all personnel authorised to access the personal health information;
- Ensuring that all personnel with access to the personal health information have signed a Confidentiality Agreement;
- Ensuring that only authorised personnel and system support staff have access to the personal health information;
- Ensuring that all authorised persons are familiar with this Practice Code and the approved protocol for the project;
- Ensuring that the project is conducted in accordance with this Practice Code and the approved protocol; and
- Giving notice of any proposed changes in the project personnel who have access to personal health information.

### 2.9 Authorised persons must:

- Comply with the Confidentiality Agreement;
- Comply with this Practice Code; and
- Conduct the project in accordance with the conditions approved by DOHWA HREC.

## 3 Use and Disclosure of Personal Health Information

**3.1** Recipients of personal health information provided by DOHWA must protect the confidentiality of the information and the privacy of the people whose information they are using. The information may only be used for limited purposes and must not be disclosed to unauthorised persons. The following guidelines must be implemented to meet these obligations.

### Restrictions on Use and Disclosure

**3.2** Health information provided by the DOHWA must only be used for the purpose specified in the Application for Data and the DOHWA HREC Application.

**3.3** Personal health information provided by the DOHWA must not be disclosed to any other institution, organisation or person other than another person authorised for the particular project.

**3.4** DOHWA information files may not be merged with other information sets held by users without approval from DOHWA HREC. Information files provided by the DOHWA for two separate projects may not be merged without approval from the relevant Data Managers and DOHWA HREC.

## Contact with Individuals

- 3.5** The information provided must not be used to attempt to identify or contact any individual.
- 3.6** If an approved use requires contact with individuals who are identified using information held by the DOHWA, then the DOHWA will make the initial contact. The DOHWA will request consent to release contact information to the researchers or invite the individual to contact the researchers.
- 3.7** The Data Managers of the relevant data collection or DOHWA HREC may require that certain conditions be met, such as an appropriate medical advisor be consulted, before initial contact is made in circumstances where there may be an unacceptable risk to the well being of the individual or their family from the initial contact.
- 3.8** The information letters and any other material sent to individuals must be approved by the DOHWA HREC.

## Obligations

- 3.9** Authorised persons must:
- Only use the information for the purpose specified in the approved Application for Data and Application for Ethical Review;
  - Not disclose any information, either original or a copy, to a person other than another person authorised for that project;
  - Not use the information to attempt to identify or make unauthorised contact with any individual; and
  - Not make any unauthorised merger with any other information set, including information files provided for two separate approved projects.

## 4 Information Security

- 4.1** A Security Plan must be developed and implemented to protect the personal health information provided by the DOHWA. The Security Plan must be specified in the application. The Security Plan should comply with the following guidelines and must be approved by DOHWA HREC and the relevant Data Managers. A checklist for Best Practice Security is provided in Appendix 1.
- 4.2** For detailed security information contact the IT Security Officer in your institution or refer to the Australian Standards for information security management on the Standards Australia website:
- AS/NZS ISO/IEC 17799:2001 Information Technology - Code of Practice for Information Security Management;
  - AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems - Requirements; (supersedes AS 7799:2:2003).

## **Electronic Records**

### **Protecting Identity**

- 4.3** Electronic records should be created and maintained so that identifying information is kept separately from other health information. Electronic records in which identifying information is juxtaposed with other health information should be created and maintained only when essential, and destroyed at the earliest opportunity.

### **Physical Security**

- 4.4** Electronic devices used to store personal health information must be kept in a secure location approved by the DOHWA HREC. This includes stand-alone, personal, or mobile computers; networked or shared computers or other electronic storage devices.
- 4.5** Physical access to that location must be securely controlled. Keys must be stored securely. Keys must not be given or loaned and no unauthorised copies of keys may be made.

### **Technological Security**

- 4.6** Access to the personal health information must be restricted by passwords.
- 4.7** Passwords must be unique to each authorised user and must not be written, e-mailed, shared or in any other way made known to anyone other than the individual user. Passwords should be changed regularly.
- 4.8** Electronic devices must be secured with automatic screen locking after 5 minutes of inactivity.
- 4.9** All personal health information must be encrypted using approved software when it is stored, transferred or archived.
- 4.10** Access to encryption keys must be restricted by password and limited to the Principal Investigator or their delegate. Encryption keys should not be stored on the same electronic device as the health information.
- 4.11** Personal health information must not be stored or processed on systems connected to the internet, or to non-secure networks, or where remote access is possible unless access is securely controlled and the remote access is restricted to authorised persons. All electronic equipment used to store or process personal health information must be protected from unauthorised external access via networks, through the use of firewalls, secure encrypted access pathways or other recommended security measures. Provision must be made for the regular update of all security protection measures.
- 4.12** All electronic devices and networks that are used must be protected from virus and other malicious software.

## **Transport**

**4.13** Where personal health information is physically transported from one approved secure location to another the following guidelines apply:

- The amount of information must be kept to a minimum,
- All information must be password protected,
- All information must be encrypted,
- Identifiers must be transported separately,
- Encryption keys should be stored on a separate device during transportation,
- The information must be transported by an authorised person, and
- The authorised person must not leave the storage device unattended.

**4.14** Personal health information must not be transmitted across unsecured networks. Transmission across networks may only be approved if they comply with the following guidelines:

- Transmission must be by approved security methods, such as Public Key Infrastructure (PKI) to protect information and authenticate users,
- Information must only be transmitted between approved secure locations,
- The amount of information must be kept to a minimum, and
- Identifiers must be transported separately.

**4.15** Data delivered to the DOHWA for linkage to other datasets must be hand delivered.

## **Paper Records**

### **Protecting Identity**

**4.16** Paper records of personal health information provided by the DOHWA, should be created only where necessary and they should be destroyed at the earliest opportunity.

**4.17** Only authorised personnel may conduct printing of paper records containing personal health information.

### **Physical Security**

**4.18** Paper records containing personal health information must only be used and stored in an approved secure location and must be stored in a locked cabinet when not in use.

**4.19** Master lists of identification numbers assigned to named individuals must be stored separately from the paper files to which they refer and must be kept in a locked cabinet in an approved secure location.

**4.20** Details of coding systems must be stored separately from records containing information in coded form and must be kept in an approved secure location.

**4.21** Proposed changes to the security or location arrangements for the personal health information must be approved by the relevant Data Managers and DOHWA HREC, where applicable. Requests for approval of modifications should be sent to the DOHWA Data Services Office.

## **Transport**

**4.22** Paper records containing personal health information provided by the DOHWA may only be transported from one location to another with express approval. The following guidelines apply:

- The amount of information must be kept to a minimum,
- The information must be transported by an authorised person, and
- The authorised person must not leave the paper records unattended during transport.

**4.23** Paper records containing personal health information provided by the DOHWA must not be transmitted by facsimile.

## **Containment of Breaches**

**4.24** All breaches of the security and confidentiality of personal health information must be reported by the Principal Investigator to the Executive Officer (EO) of DOHWA HREC immediately.

**4.25** In the event of a breach the person who discovers the breach should immediately initiate a process of containment to prevent further release of information. The containment process should:

- Determine what if any information has been disclosed,
- Retrieve as much information as possible,
- Ensure no copies of the personal health information have been made or retained by an unauthorised person,
- Ensure that additional breaches cannot occur through the same means,
- Determine whether the breach will enable access to any other personal health information and take whatever steps are necessary to prevent it, and
- Ensure that there is no further harm or damage to participants.

## **Obligations**

**4.26** The Principal Investigator is responsible for:

- Ensuring that all personnel are familiar with the requirements of the approved Security Plan;
- Ensuring that the project is conducted in compliance with the approved Security Plan;
- Obtaining approval from DOHWA HREC for any proposed changes to the Security Plan; and
- Notifying the EO of DOHWA HREC immediately of any breach of security of the information.

#### **4.27** Authorised Persons are responsible for:

- Conducting the project in compliance with the Security Plan;
- Containing any breach of the security of the information; and
- Notifying the Principal Investigator or the EO of DOHWA HREC of any breach of security of the information.

## **5 Information Retention and Disposal**

**5.1** Personal health information should be retained only as long as is necessary for the conduct and the validation of the research or analysis. Applicants must specify a plan for the retention and disposal of the information. The Retention and Disposal Plan should comply with following guidelines and must be approved by DOHWA HREC and the relevant Data Managers.

### **Retention**

**5.2** The Retention and Disposal Plan must specify the period during which personal health information will be retained after completion of the project. Personal health information may only be retained for validation or for approved extensions of the work.

**5.3** The location and security arrangements for archived information must be approved.

**5.4** The security guidelines apply to any period during which the personal health information is retained.

**5.5** Files containing personal health information retained for validation or for approved extensions of the work must be encrypted using approved software.

**5.6** The Data Managers of the relevant data collections must be notified that all retained files have been encrypted and the custodian of the encryption key must be nominated. Notifications should be sent to the Data Service Office.

**5.7** The personal health information retained in archives should be reduced to the minimum necessary for validation.

### **Disposal**

**5.8** The Retention and Disposal Plan must specify the date by which all personal health information will be destroyed.

**5.9** The Data Managers of the relevant data collections must be notified when the destruction of the information is complete. Notifications should be sent to the Data Service Office.

**5.10** Destruction of the information means that any personal health information either in its original form or any derived form in paper, electronic, or any other storage medium including back-up copies will no longer exist.

**5.11** All derived forms of information must be identified and destroyed.

- 5.12** All temporary files must be destroyed on completion of the project
- 5.13** Electronic devices used to store information retained for validation or for approved extensions of the work must be sanitised and all files must be destroyed by the approved destruction date. For appropriate sanitisation methods, refer to the *Australian Government Information and Communications Technology Security Manual (ACSI 33), Part 3- Chapter 4*. ACSI 33 is available from the Defence Signals Directorate of the Australian Government Department of Defence
- 5.14** Electronic devices used to store personal health information during the project must be sanitised at the end of the project and all files deleted in such a way that the contents of the files, and not just the directory entries, are destroyed.
- 5.15** Electronic devices used to hold personal health information provided by the DOHWA must be thoroughly sanitised before being reassigned to, or used by, persons other than those authorised by DOHWA HREC.
- 5.16** Paper records containing personal health information must be shredded for disposal. Disposal should be carried out on the research site. If disposal off site is necessary then an authorised member of the research team must supervise the disposal.

### **Obligations:**

- 5.17** The Principal Investigator is responsible for:
- Ensuring that the project is conducted in compliance with the approved Retention and Disposal Plan;
  - Obtaining approval for any proposed changes to the Retention and Disposal Plan;
  - Providing notice that all retained files have been encrypted and nominating the custodian of the encryption key;
  - Providing notice when the destruction of the information is complete; and
  - Notifying the DOHWA Data Services Office of any breaches of the approved Retention and Disposal Plan.
- 5.18** Authorised persons must:
- Conduct any tasks relating to the retention and disposal of the information in accordance with the approved Retention and Disposal Plan; and
  - Notify the Principal Investigator or the DOHWA Data Services Office of any breaches of the approved Retention and Disposal Plan.

## **6 Reporting and Monitoring**

- 6.1** The Data Managers of the data collections and DOHWA HREC are required to maintain records, monitor and report on the use of information provided by the DOHWA. The following guidelines outline the reporting requirements for users of information provided by the DOHWA. Forms are provided to assist users to meet their reporting obligations. All reports, notifications and requests for amendments should be sent to the DOHWA Data Services Office, which will forward them to the relevant Data Managers and to the EO of DOHWA HREC as required.

### **Monitoring Reports**

- 6.2** DOHWA HREC will monitor projects it approves and projects approved by the Confidentiality of Health Information Committee and will require the submission of periodic reports on the progress of the project. The minimum requirement is for the submission of an Annual Report describing the progress of the project and a Final Report on completion of the project. The project approval may specify other periodic reporting requirements. Continuing approval of all projects is subject to the Principal Investigator meeting the approved reporting requirements.
- 6.3** The Data Managers and DOHWA HREC may each request additional information, conduct random checks or adopt any additional mechanism deemed appropriate to monitor compliance of projects they have approved.

### **Modifications to Approved Projects**

- 6.4** All modifications to a project must be approved by the relevant Data Managers and by DOHWA HREC. This includes changes to:
- Personnel working on the project,
  - The Security Plan,
  - The Retention and Disposal Plan, and
  - Changes to the research methodology.

Requests for approval of modifications to a project should be sent to the DOHWA Data Services Office.

- 6.5** Notification must be given to the DOHWA Data Services Office if a project is suspended or ceases.

### **Retention and Destruction of Information**

- 6.6** Notification must be given to the DOHWA Data Services Office when all retained files have been encrypted and the custodian of the encryption key must be nominated.
- 6.7** Notification must be given to the DOHWA Data Services Office of the final destruction of all the personal health information.

## Breaches, Complaints and Adverse Events

**6.8** The following matters must be reported immediately:

- Breaches of the approved protocol,
  - Complaints about the conduct of a project,
  - Adverse events, and
  - Any unforeseen events that might affect the ethical acceptability of the project.
- Reports should be sent to the EO of DOHWA HREC.

**6.9** The procedures and consequences for dealing with these matters are outlined in DOHWA HREC *Standard Operating Procedures No's 17, 18 and 19*.

### Obligations:

**6.10** The Principal Investigator is responsible for:

- Ensuring that annual reports are submitted by the due date;
- Ensuring that all monitoring reports are submitted in a timely manner;
- Ensuring that approval is sought for all proposed modifications to the project protocol;
- Providing notifications relating to storage and destruction of information; and
- Providing notification of the suspension or cessation of a project.

**6.11** Authorised persons are responsible for:

- Reporting all breaches, complaints, adverse events or other relevant changes in circumstances to the Principal Investigator or the EO of DOHWA HREC immediately.

## 7 Publication

**7.1** The public interest is promoted by the publication of research results. However, the privacy of individuals should be protected. These guidelines govern the publication of research results.

**7.2** The results of all research using information provided by the DOHWA to external applicants should be published as soon as possible.

**7.3** Individuals or health care providers must not be identified or identifiable in publications of any kind unless they have given written consent. (Contact must be made in compliance with 3.6).

**7.4** All manuscripts, reports or other proposed publications based on analysis of information provided by the DOHWA must accurately describe the data collections and linkage methods.

**7.5** The Data Managers may require that all manuscripts submitted for publication be provided to the Data Managers for comment at the time of submission for publication so that the Data Managers can audit compliance with paragraph 7.3

and 7.4. The Data Managers will notify the Principal Investigator of any breach of confidentiality or inaccuracies in the description of resources so that the manuscript can be modified to comply with these requirements.

**7.6** All publications must acknowledge the use of information provided by the DOHWA and the use of linkages provided by Data Linkage Branch.

**7.7** The DOHWA must be informed of all publications and reports of the results of the research using information provided by the DOHWA. Notifications should be sent to the DOHWA Data Services Office and included in the final Report to DOHWA HREC.

### **Obligations:**

**7.8** The Principal Investigator is responsible for:

- Ensuring that the research results are published as soon as possible;
- Providing the relevant DOHWA Data Managers with copies of all manuscripts for comment prior to submission for publication; and
- Notifying the DOHWA Data Managers of all publications, presentations and reports of the results of the research.

## **Acknowledgments**

The Confidentiality of Health Statistics Committee published the first Code of Practice for Use of Identified Data from the Department of Health Statistical Data Collections in 1986. Its successor, the Confidentiality of Health Information Committee (CHIC), revised the code in 1994 and 2002. This Practice Code is based on these earlier documents.

Ms Myra Cake carried out a review of the existing Code and wrote the initial drafts of this Practice Code. The Department of Health gratefully acknowledges her contribution. The Department of Health also gratefully acknowledges the assistance of Dr David Blackledge, the chair of CHIC, and Dr Judith Finn, a past member of CHIC in development of the Practice Code.

The Practice Code has been based on a review of the privacy and security policies of a number of other institutions including the Institute for Clinical Evaluative Services, Toronto; the Canadian Institute for Health Information, Ottawa; the Manitoba Centre for Health Policy, University of Manitoba; and the US Department of Health and Human Services.

## Appendix 1

### Checklist for Best Practice Security

#### Protecting Identity

- Separate storage of identifying information and other health information

#### Physical Security

- Locked
- Access restricted

#### Technological Security

- Password protected
- Automatic locking
- Encrypted
- Firewall protected
- Virus and spyware protected

#### Transport

- Approved
- Minimum necessary
- Password protected
- Encrypted
- Identifiers and encryption keys separated
- By authorised person
- Kept with the person at all times

#### Retention

- Specified period
- Secure location
- Encrypted

#### Disposal

- All files, copies, disks and devices to be physically destroyed or sanitized

#### **For further detailed technical information security information:**

- Contact the IT Security Officer in your institution; or
- Refer to the following standards for information security management available from Standards Australia:
  - AS/NZS 17799:2001 Information Technology - Code of Practice for Information Security Management;
  - AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems - Requirements; (supersedes AS 7799:2:2003).

# Delivering a Healthy WA

