Government of **Western Australia**
Department of **Health**

Information Circular

Enquiries to: Brooke Smith
Senior Policy Officer

Phone number: 9222 0268

IC number: 0177/14

Date: March 2014
Supersedes:
File No: F-AA-23386

Subject: **Practice Code for the Use of Personal Health Information Provided by the Department of Health**

WA Health collects, stores, uses and discloses large volumes of data. Information is an important resource used for the clinical care of patients, for funding, management, planning, monitoring, improvement, research and evaluation of health and health services in the State.

WA Health is committed to ensuring that information supporting the provision of health care is readily available to authorised users, when and where it is needed. Users of WA Health information are required to utilise this resource in a responsible, ethical and lawful manner. The *Practice Code for the Use of Personal Health Information Provided by the Department of Health* (Practice Code) establishes guidelines applicable to authorised users of personal health information that has been provided by the Department of Health. It ensures that the personal health information is used in a manner that respects the sensitive nature of the information and the privacy of the people that it relates to.

The Practice Code outlines the minimum standards and principles that must be followed when obtaining, handling, using, storing and disposing of personal health information.

Colin Xanthis
DIRECTOR, PERFORMANCE
PERFORMANCE ACTIVITY AND QUALITY
DEPARTMENT OF HEALTH

This information is available in alternative formats on request from a person with disability.

Government of Western Australia
Department of Health

PRACTICE CODE

FOR THE USE OF PERSONAL HEALTH INFORMATION PROVIDED BY THE DEPARTMENT OF HEALTH

CONTENTS

TITLE: PRACTICE CODE FOR THE USE OF PERSONAL HEALTH INFORMATION PROVIDED BY THE DEPARTMENT OF HEALTH

1. BACKGROUND

WA Health creates and collects a vast amount of information on behalf of the people of Western Australia. The health information that is maintained by the Department of Health (the Department) contains personal health information. Personal health information relates to details about an individual whose identity is apparent or can reasonably be ascertained from that information. Personal health information is confidential and may be particularly sensitive. The information is used for, but not limited to, funding, management, planning, monitoring, improvement and evaluation of health and health services as well as for research purposes.

The *Practice Code for the Use of Personal Health Information Provided by the Department of Health* (Practice Code) is a practical guide outlining the minimum[1] standards and principles to be followed when obtaining, handling, using, storing and disposing of personal health information provided by the Department. For the purpose of this document, the Department refers to the Department of Health Divisions and excludes the Health Services (Child and Adolescent Health Service, North Metropolitan Health Service, South Metropolitan Health Service and WA Country Health Service).

The Department is committed to ensuring the information that supports the provision of health care services is readily available to authorised users[2], when and where it is needed; however, confidential information must also be protected from unauthorised use. The Practice Code ensures that authorised users of personal health information provided by the Department use it in a manner that respects the sensitive nature of the information and the privacy of the people that it relates to. It also provides a consistent approach to managing the use of personal health information provided by the Department.

The Department has a responsibility under *The Western Australian Public Sector Code of Ethics* to use its resources in a responsible and accountable manner that ensures the efficient, effective and appropriate use of information. The Practice Code aims to provide appropriate protections for legitimate use of personal health information provided by the Department.

2. POLICY

The Practice Code is applicable to:

- all personal health information held by the Department, including those held in the Department's data collections (e.g. Hospital Morbidity Data System, Emergency Department Data Collection, Western Australian Cancer Registry)
- authorised users of personal health information that has been provided by the Department (linked[3] or otherwise) for the purposes of funding, management,

[1] Data Custodians may require additional standards or conditions for some Department of Health data collections, such as appointment of an appropriate medical advisor.
[2] An authorised user is a person who has obtained the appropriate approvals for the use of Department of Health information. The appropriate approvals are determined from the Information Access and Disclosure models (refer to *Information Access and Disclosure Policy OD 0360/12*) for each data collection, that has been endorsed by the Data Steward and acted upon by the Data Custodians. The authorised user includes those employed by the Department, the Health Services, other State or Commonwealth agencies, and all other users.
[3] Linkages created within and between data sources for information that is thought to relate to the same person, family, place or event.

planning, monitoring, improvement or evaluation of health services, training, research, compilation or analysis of statistics in the public interest.

The Practice Code is not applicable:

- to staff within the Department authorised to access personal health information, unless their work requires the establishment of new linkages with data collections held by the Department
- where information is required to meet mandatory reporting[4] obligations or clinical patient management requirements.

The principles and guidelines outlined in this Practice Code are the minimum requirements for users to apply.

3. PERSONAL HEALTH INFORMATION

Personal health information includes details about an individual whose identity is apparent or can reasonably be ascertained from that information. It includes both identifying information (e.g. name, address, date of birth, medical record number) and health information (e.g. diagnosis, treatment).

Control mechanisms based on assessed risks, benefits to the community, ethical considerations and legal requirements must be in place for managing access and disclosure of personal health information.

The Department of Health WA Human Research Ethics Committee (DOH HREC) has ethical responsibility for oversight of the use and disclosure of personal health information held in the Department's data collections. Requests within scope, for the use of personal health information (linked or otherwise) from the Department's data collections require approval from DOH HREC.[5]

3.1 Principles in the Use of Personal Health Information

Principles for the appropriate use of personal health information provided by the Department and for protecting the privacy of people that it relates to are:

Principle 1	•The information must only be used for the authorised purpose.
Principle 2	•The information must only be used by authorised person(s) for the authorised purpose.
Principle 3	•The information must be protected by appropriate and approved security measures at all times.
Principle 4	•The information must not be further disclosed to any other institution, organisation or person(s) without prior approval from the Data Custodian(s) and DOH HREC.
Principle 5	•The information must not be merged with any other information sets held by the user without prior approval from the Data Custodian(s) and DOH HREC.

[4] Mandatory reporting refers to information required under the National Healthcare Agreement, National Health Reform Agreement or any other funding agreements or information required under legislation.

[5] Refer to the Department of Health WA Human Research Ethics Committee Terms of Reference for further information about projects that are within scope of the committee. Appropriate approvals are also determined from the Information Access and Disclosure models (refer to *Information Access and Disclosure Policy OD 0360/12*) for each data collection, that has been endorsed by the Data Steward and acted upon by the Data Custodians.

Principle 6	•The information must not be used to identify or contact any individual unless this is an approved purpose.[6]
Principle 7	•The information must not be kept for longer than approved by the Data Custodian(s) and DOH HREC.
Principle 8	•At the end of the approved retention period the information must be disposed of securely and completely.

4. SECURITY OF PERSONAL HEALTH INFORMATION

Principal Investigators receiving personal health information provided by the Department must take steps that are reasonable to ensure that personal health information is:

- protected against theft, loss and unauthorised access, use or disclosure
- protected against unauthorised copying or modification
- retained, transferred and disposed of in a secure manner.

A security plan must be developed, approved by the Data Custodian(s) and DOH HREC and implemented to protect the personal health information provided by the Department. The security plan should address the following for both electronic and paper records:

- protecting identity
- physical and technological security
- transport.

The Department may request an audit or inspection of the security arrangements outlined in the security plan.

Proposed changes to the security or location arrangements for personal health information must be approved by the Data Custodian(s) and DOH HREC.

The following guidelines are the minimum requirements for ensuring personal health information provided by the Department is secure and protected. A *Checklist for Best Practice Security* is provided in Appendix 1 to assist with applying the security measures below.

Electronic Records

4.1 Protecting Identity

a) Electronic records should be created and maintained so that identifying information is kept independently of health information.
b) Access to identifying information should be minimised.
c) Electronic records in which identifying information is juxtaposed with other personal health information should be created and maintained only when essential and approved by the Data Custodian(s) and DOH HREC, then destroyed at the earliest opportunity.
d) Active measures must be taken to prevent unauthorised persons from overhearing, seeing or accessing personal health information.
e) Measures must be taken to ensure separation of roles between the data system administrator, data linkage officer and analysts (refer to section 11.1).

[6] If an approved use requires contact with individuals who are identified using information held by the Department of Health, then the Department will make the initial contact. The Department of Health will request consent to release contact information to the Principal Investigator or invite the individual to make contact with the Principal Investigator.

4.2 Physical Security

a) Physical access controls should be in place to prevent unauthorised access to hardware, network media and data storage media.
b) Physical access control credentials should be appropriately managed.
c) Electronic devices used to store personal health information must be kept in a secure location approved by the Data Custodian(s) and DOH HREC. This includes stand-alone, personal, or mobile computers, networked or shared computers and any other electronic storage devices.
d) Workstations should be positioned to prevent unauthorised access to equipment or viewing of information displayed on screens.

4.3 Technological Security

a) Electronic devices and computer networks containing personal health information provided by the Department must be protected by password logons to prevent unauthorised access.
b) 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 authorised user.
c) Passwords should be changed regularly.
d) Electronic devices must be signed out of, or workstation locked when not in use or left unattended, even briefly. Electronic devices must also be secured with an automatic screen locking mechanism after 10 minutes of inactivity.
e) All personal health information must be encrypted using appropriate software when it is stored, archived or transferred.
f) Access to encryption keys must be restricted by passwords and limited to the Principal Investigator or their authorised delegate. Encryption keys should not be stored on the same electronic device as the personal health information.
g) Personal health information must not be stored or processed on systems connected directly to a non-secure network or where remote access is possible, unless access is securely controlled and the remote access is restricted to authorised personnel only.
h) 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.
i) All electronic devices and networks that are used must be protected from viruses and other malicious software.

4.4 Transport

a) 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
    - the authorised person must not leave the storage device unattended.
b) Personal health information must not be transmitted across any unsecured network. Electronic transmission of personal health information is prohibited unless it is encrypted and complies with the following guidelines:

- transmission must be by approved security methods, such as Public Key Infrastructure 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
- identifiers must be transmitted separately
- transmission is via secure file transfer protocol.

c) Personal health information must not be transported overseas without consultation with the Data Custodian(s) and subsequent approval from the Data Steward and DOH HREC. The Data Custodian(s) may seek legal advice before referring the request to the Data Steward for endorsement.

Paper Records

4.5 Protecting Identity

a) Paper records of personal health information provided by the Department should be created only where necessary and should be destroyed at the earliest opportunity.
b) Only authorised personnel may conduct printing of paper records containing personal health information.
c) Access to identifying information should be minimised.
d) Measures must be taken to ensure separation of roles between the data system administrator, data linkage officer and analysts (refer to section 11.1).

4.6 Physical Security

a) 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.
b) Keys must be stored securely and must not be given or loaned and no unauthorised copies of keys may be made.
c) 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.
d) Details of coding systems must be stored separately from records containing personal health information in coded form and must be kept in a locked cabinet in an approved secure location.

4.7 Transport

a) Paper records containing personal health information provided by the Department may only be transported from one location to another with approval from the Data Custodian(s) and DOH HREC. The following guidelines apply:
   - the amount of information must be kept to a minimum
   - the information must be transported by an authorised person
   - the authorised person must not leave the paper records unattended during transport.
b) Paper records containing personal health information provided by the Department must not be transmitted by facsimile.

5. INFORMATION RETENTION AND DISPOSAL

A Retention and Disposal Plan must be developed and approved by the Data Custodian(s) and DOH HREC and should comply with the following guidelines.

5.1 Retention

a) Personal health information should be retained only as long as necessary and the retention period must be approved by the Data Custodian(s) and DOH HREC.
b) Personal health information retained in archives should be reduced to the minimum necessary for validation.
c) The location and security arrangements for archived personal health information must be approved by the Data Custodian(s) and DOH HREC.
d) The information security guidelines apply to any period during which the personal health information is retained.
e) Electronic files containing personal health information retained for validation or for approved extensions of the work must be encrypted.
f) A custodian of the encryption key must be nominated.

5.2 Disposal

a) The *Retention and Disposal Plan* must specify the date by which all personal health information provided by the Department will be destroyed.
b) The Data Custodian(s) and DOH HREC must be notified of the following details when the destruction of the personal health information is complete:
   - the title of the project/information
   - when it was destroyed
   - how it was destroyed
   - who destroyed it
   - who approved the destruction.
c) Destruction of the personal health information provided by the Department 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.
d) Electronic devices used to store personal health information must be sanitised and all files deleted in such a way that the contents of the files, and not just the directory entries, are destroyed. For appropriate sanitisation methods, refer to the WA State Records Office publication *Sanitizing Digital Media and Devices Guideline*.
e) Paper records containing personal health information must be shredded or pulped for disposal.
f) Disposal should be carried out at the approved location and if disposal is off site it is necessary that an authorised person supervises the disposal.

6. REPORTING AND MONITORING

Data Custodians and DOH HREC are required to maintain records, monitor and report on the use of personal health information provided by the Department. Users of personal health information provided by the Department are required to provide the following:

- monitoring reports
- advice of modifications.

6.1 Monitoring Reports

a) Periodic progress reports must be submitted to the Data Custodian(s) and DOH HREC. The minimum requirements are for the submission of an *Annual Progress Report* describing the progress in the use of personal health information provided by the Department and a *Final Report* once the use of information is complete.
b) Approval for the use of personal health information provided by the Department may include additional reporting requirements and continuation for the use of information is subject to the Principal Investigator meeting the approved conditions.

c) The Data Custodian(s) and DOH HREC may at any time request additional information, conduct random checks or adopt any additional mechanism deemed appropriate to monitor compliance.

6.2 Modifications

a) All modifications to a project must be approved by the Data Custodian(s) and DOH HREC. This includes, but is not limited to, changes to the:
   - approved purpose/protocol
   - participant information or consent forms
   - contact details
   - project personnel
   - security plan
   - retention and disposal plan.

b) Notification must be given to the Data Custodian(s) and DOH HREC if the use of personal health information provided by the Department is suspended or ceases.

7. BREACHES, COMPLAINTS AND ADVERSE EVENTS

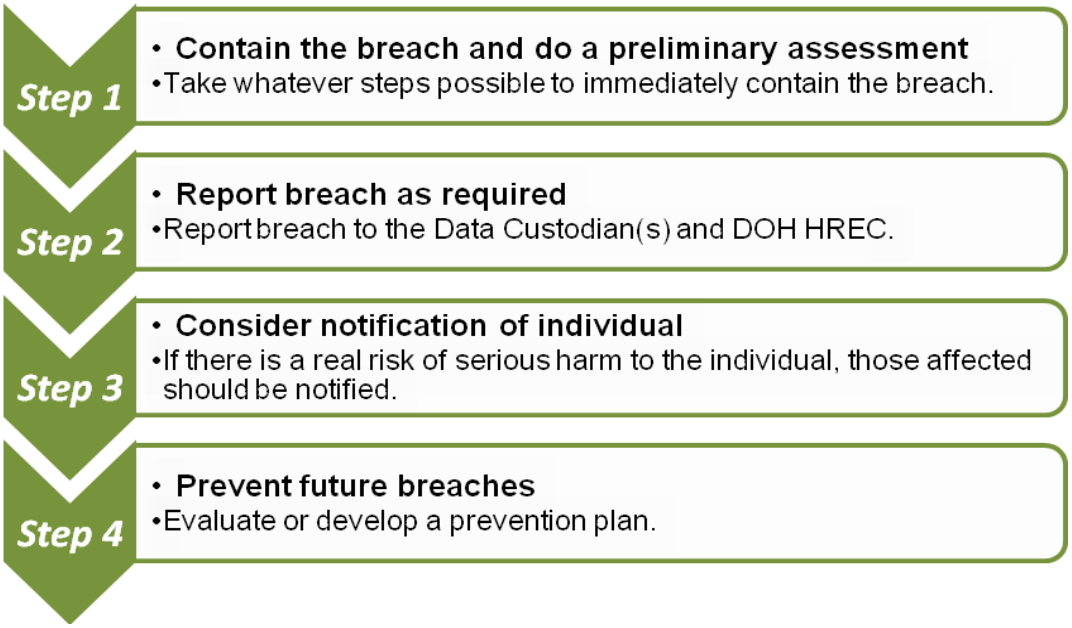
Breaches, complaints and adverse events can be caused by a variety of factors, affect different types of personal health information and give rise to a range of actual or potential harm to individuals, agencies and organisations.

Given this context, there is no single way of responding to breaches, complaints and adverse events. Each event will need to be dealt with on a case-by-case basis, undertaking an assessment of the risks involved, and using that risk assessment as the basis for deciding what actions to take in the circumstances.

The following matters must be reported to the Data Custodian(s) and DOH HREC immediately:

- breaches of the approved use of personal health information
- complaints on the conduct of the use of personal health information
- adverse events - any unforeseen events that may affect the ethical acceptability of the use of the personal health information provided by the Department.

There are four key steps to consider when responding to a breach or suspected breach:



7.1 Breaches

The following guidelines should be followed in the case of a breach or suspected breach:

a) All breaches or suspected breaches of the security and confidentiality of personal health information must be reported to the Data Custodian(s) and DOH HREC immediately. Appendix 2 contains a *Breach Incident Form* for completion if a breach has been identified or is suspected.

b) In the event of a breach the person who discovers the breach should immediately initiate a process of containment. The containment process should:

- determine what (if any) personal health information has been disclosed
- retrieve as much personal health 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
- ensure that there is no further harm or damage to individuals.

7.2 Complaints and Adverse Events

The following guideline should be followed in the case of any complaints about conduct in the use of personal health information provided by the Department and any adverse events:

a) Complaints or adverse events must be reported to the Data Custodian(s) and DOH HREC immediately.

Following contact regarding an incident, the Data Custodian(s) will decide the procedures and consequences for dealing with these matters.

DOH HREC procedures and consequences are outlined in the *Standard Operating Procedures*.

7.3 Consequences of Breaches

The possible consequences of breaches include:

- notation on the DOH HREC project file of the occurrence of the breach
- increased monitoring of the project by DOH HREC and Data Custodian
- further training and education on security practices
- amendments to the approved research protocol
- suspension or cancellation of DOH HREC approval of the project (with the immediate return or destruction of all data files)
- exclusion of particular individuals responsible for the breach from future access to personal health information provided by the Department either for a period of time or indefinitely
- reporting the individuals responsible for the breach to their employer, with a complaint of misconduct in the conduct of the project
- reporting the individual responsible for the breach to the funding agency that has supported the project, with a complaint of misconduct
- reporting the individual responsible for the breach to any external agency with jurisdiction (such as professional registration board or the Privacy and Information Commissioner), with a complaint of misconduct
- reporting allegations of criminal conduct to the police.

8. PUBLICATION

The public interest is promoted by the publication of research results and reports following the analysis of personal health information provided by the Department. However, the privacy of individuals must be protected. The following guidelines govern the publication of results:

a) Individuals or health care providers must not be identified or be identifiable in publications of any kind unless they have given written consent (contact must be in compliance with Principle 6). This may require suppression of small numbers. Small numbers may identify persons in a publication, particularly if the person is within a small population.
b) The Data Custodian(s) and DOH HREC must be informed of all draft publications, presentations and reports resulting from the use of personal health information provided by the Department.
c) The Data Custodian(s) may require that manuscripts be submitted to the Data Custodian(s) before publication for audit and compliance with paragraphs 7(a) and (d).
d) All manuscripts, reports or other proposed publications based on analysis of personal health information provided by the Department must accurately describe the data collections and data linkage methods.
e) The results of all research and analysis using personal health information provided by the Department to external users should be published as soon as possible.

9. CONTACT INFORMATION

9.1 Department of Health WA Human Research Ethics Committee

The following contact details are for DOH HREC.

Level 1, C Block, 189 Royal Street, EAST PERTH WA 6004
Executive Officer: (08) 9222 4278
Fax: (08) 9222 2396
Email: HREC@health.wa.gov.au
Web: http://www.health.wa.gov.au/healthdata/HREC/index.cfm

9.2 Health Data Custodians

The following contact details are for the core health data collections within the Department.

Level 1, C Block, 189 Royal Street, EAST PERTH WA 6004
Telephone: (08) 9222 2073
Fax: (08) 9222 2396
Web: http://www.health.wa.gov.au/healthdata/contact/index.cfm

10. DEFINITIONS

Authorised User	is a person who has obtained the appropriate approvals for the use of Department of Health information and has signed a declaration of confidentiality for the use of personal health information provided for the particular project.
Data Collection	is a systematic gathering of data for a particular purpose from various sources, including manual entry into an information system, questionnaires, interviews, observation, existing records and electronic devices. This includes both operational data collections and data repositories.
Data Custodian	is responsible for the day-to-day management of data from a business perspective. The Data Custodian aims to improve the accuracy, usability and accessibility of data within the data collection.
Data Steward	is the delegate with the responsibility for setting the overall strategic direction of the specific data collection to ensure the collection is developed, maintained and utilised in accordance with the strategic goals of WA Health.
Data Linkage	is the activity of finding connections between different pieces of information that are thought to belong to the same person, family, place or event.
Identifiable	information is where the identity of an individual or health provider can be reasonably ascertained by the holder of the information: examples of identifiers include: name, address, full date of birth, geocodes, hospital names or numbers. an individual will be identifiable if the information contains unique personal identifiers and the holder of the information also has the master list linking the identifiers to individuals. it may be possible to ascertain the identity of individuals from aggregated data where there are very few individuals in a particular category.
Information Access	refers to the direct access by end users (both internal and external to the Department) to information within an organisation. Typically, direct access is gained via a network and/or system login and password to a front-end information system or to a back-end database.
Information Disclosure	refers to the release of information to end users (both internal and external to the Department) from data collections or paper based records within an organisation. Information is generally released in the form of hard copy documents, data extracts or electronic medium.
Network (Computer)	is made up of a collection of hardware and software components interconnected by communication channels that allow sharing of resources and information, such as: Local Area Network (LAN) – a network that connects computers and devices in a limited geographical area, for

	example: home, work, school. Wide Area Network (WAN) – a network that covers a large geographic area, for example: city, country or intercontinental. Internet – a network which is a global system of interconnected governmental, academic, corporate, public and private computer networks.
Personal Health Information	includes details about an individual whose identity is apparent or can reasonably be ascertained by the holder of the information either from the information itself or by using other information that they already hold.
Principal Investigator	is the person who has ultimate responsibility in managing the use of the personal health information.

11. ROLES AND RESPONSIBILITIES

All personnel who are authorised to use personal health information provided by the Department are bound by duties of confidentiality and legal obligations to protect the privacy of the individuals whose information is being used. Personnel who are external to WA Health will be required to sign a declaration of confidentiality before the release of personal health information. The declaration for confidentiality is available on the DOH HREC website (refer to HREC006 – Confidentiality Agreement for Researchers).

Every application for access to personal health information held in the Department's data collections must nominate a Principal Investigator who is responsible for compliance with this Practice Code and the protocol and conditions for the project approved by DOH HREC. The Principal Investigator must be the person who has the ultimate responsibility for the management of the project. This is not necessarily the same person as the Chief Investigator named on any funding grants. The Principal Investigator must be sufficiently senior to undertake the obligations outlined in this Practice Code and is required to take personal responsibility for the management of the project and the reporting requirements. Where the application is made for a student project the Principal Investigator should be the student's supervisor.

Table 1 outlines the roles and minimum responsibilities for the provision and use of personal health information provided by the Department.

Roles	Responsibilities
Data Custodian(s)	• Considers requests for personal health information. • Specifies conditions for the use of personal health information. • Ensures that the purpose of the request cannot reasonably be accomplished unless personal health information is disclosed. • Ensures access is permitted on a need-to-know basis only. • Reviews the Security Plan provided by the Principal Investigator.

Data Custodians (cont.)	• Reviews access approvals regularly to ensure validity. • Maintains records on the use of personal health information provided. • Considers requests for modifications to the original request and plans. • Assesses any action to be taken in the event of a personal health information breach, complaint or adverse event.
Principal Investigator	• Has ultimate responsibility for the management, including security and protection of privacy, of personal health information provided by the Department and entrusted to their care. • Must ensure compliance with any conditions, including observance of this Practice Code, imposed by the Data Custodian(s) and DOH HREC. • Has responsibility for all monitoring and reporting requirements. • Must ensure all personnel (including data and system administrators) who will use or have access to the personal health information are authorised users and have signed a declaration of confidentiality where applicable. • Must strictly limit access to identified information to only those authorised users who need to use that information for their work. • Must limit use of the data to its approved purpose. • Must declare any conflict of interest (if applicable) whether it is commercial, financial, intellectual or other. • Must provide notification of any changes to authorised personnel who have access to personal health information provided by the Department. • Must consult with the Data Custodian(s) and obtain Data Steward and DOH HREC approval before transporting personal health information overseas. • Must only retain personal health information as long as approved in the Retention and Disposal Plan. • Must apply to the Data Custodian(s) and DOH HREC to modify any conditions or requirements of use of personal health information. • Must report immediately to the Data Custodian(s) and DOH HREC in the event of any personal health information breach, complaint or adverse event. • Must inform the Data Custodian(s) and DOH HREC of all draft publications, presentations and reports resulting from the use of personal health information.

Authorised Data User (for example: Research Team)	• Must comply with any conditions imposed by the Data Custodian(s) and DOH HREC. • Must sign and comply with the declaration of confidentiality where applicable. • Must comply with this Practice Code and only use the data for its approved purpose.
Department of Health WA Human Research Ethics Committee	• Promotes the ethical use of personal health information. • Promotes ethical standards for human research. • Protects the welfare, rights and dignity of individuals. • Assists ethical research through efficient and effective review processes. • Assess and provides ethical approval for the use of personal health information.

11.1 Minimisation and Separation of Roles

The Principal Investigator has ultimate accountability for the data sets received, including ensuring staff compliance both with confidentiality requirements and with conditions of use set out by the Data Custodian(s) and DOH HREC. The Principal Investigator is responsible for the security of personal health information and for protecting the privacy of individuals whose information is contained in the data sets.

As the guardian of the data entrusted to their care they must ensure that protocols required to protect privacy are implemented. Examples of measures to take include:

- strictly limiting access to identified information to only those authorised personnel who need to use that information for their work
- ensuring data sets used for analysis do not contain identifying data
- ensuring personnel have access only to the data required for their work
- ensuring technical personnel (data and system administrators) are aware of their obligations regarding access to data.

The risk of re-identifying data that does not contain identifiers should be minimised as much as possible.

Examples of measures to take include:

- ensuring collectors of identified information (e.g. data extracted from medical records) do not analyse the data
- ensuring the person responsible for managing the identifying data (e.g. data and system administrator) is not a data user themselves (separation of roles).

12. ASSOCIATED WA HEALTH INFORMATION

Acceptable Use Standard – Computing and Communications Facilities (OD 0114/08)

Data Stewardship and Custodianship Policy (OD 0231/11)

Information Access and Disclosure Policy (OD 0360/12)

Information Classification Policy (OD 0304/10)

Information Lifecycle Management Policy (OD 0371/12)

Information Security Policy (OD 0389/12)

Information Use Policy (OD 0390/12)

WA Health Code of Conduct (OD 0383/12)

13. RELEVANT LEGISLATION

Privacy Act 1988
Public Sector Management Act 1994

14. AUSTRALIAN STANDARDS

AS/NZS ISO/IEC 27002:2006	*Information Technology – Security Techniques – Code of Practice for Information Security Management*
AS/NZS ISO/IEC 27001:2006	*Information Technology – Security Techniques – Information Security Management Systems – Requirements*
AS ISO 2779-2011	*Information Security Management in Health Using ISO/IEC 27002*

15. OTHER RELATED DOCUMENTS

Government of Newfoundland and Labrador. 2011. *The Personal Health Information Act Policy Development Manual.* http://www.health.gov.nl.ca/health/phia/phia_policy_development_manual_feb_2011.pdf

National Health and Medical Research Council. 2007. *National Statement on Ethical Conduct in Human Research.* http://www.nhmrc.gov.au/guidelines/publications/e72

Public Sector Commission of Western Australia. 2012. *Public Sector Commission Code of Ethics*. http://www.publicsector.wa.gov.au/public-administration/official-conduct-and-integrity/code-ethics

State Records Office of Western Australia. 2011. *Sanitizing Digital Media and Devices.* http://www.sro.wa.gov.au/sites/default/files/sanitizing_media_July_2011.pdf

APPENDIX 1

CHECKLIST FOR BEST PRACTICE SECURITY

Protecting Identity

☐ Separate secure storage of identifying information and health information
☐ Separation of functions: data custodianship, linkage and analysis
☐ Statistical disclosure controls

Physical Security

☐ Locked
☐ Secure location
☐ Access restricted

Technological Security

☐ Password protected [minimum length, mix of characters etc]
☐ Automatic screen locking [after ≤10 minutes of inactivity]
☐ Encrypted
☐ Firewall protected
☐ Virus and spyware protected

Transport

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

Retention

☐ Specified period
☐ Secure location
☐ Encrypted

Disposal

☐ All files, copies, disks and devices to be physically destroyed or sanitized as per the State Records Office Sanitizing Digital Media and Devices Guideline
☐ Data Custodian(s) and DOH HREC to be notified

APPENDIX 2

BREACH INCIDENT REPORT FORM

For submission to the relevant Data Custodian(s) and DOH HREC.

Background Information:

Full name	
Contact Information	
Reference number (issued by DOH HREC, Data Custodian, etc.)	

Details of Incident:

Date of occurrence	
Date discovered	
How was it discovered?	
Description of incident	
Estimated number of individuals affected	
Description of action taken to contain breach	
Was the affected party(ies) notified of the incident? **If so, what was the date of notification?**	
Was anyone else notified of the incident (i.e. health service, university etc.)? **If so, who and when were they notified?**	

Signature Date

This document is available in different formats, upon request from a person with disability.