Government of Western Australia
Department of Health
Health Information Network

INFORMATION SECURITY POLICY

1. PURPOSE

To support the protection of WA Health's information from unauthorised access, use, disclosure, modification, or destruction throughout the information lifecycle.

2. SCOPE

The scope of this policy includes all WA Health information held in any format or medium. Information security methods must be commensurate with the sensitivity of the information and be in accordance with the security levels defined in the *Information Classification Policy.*

This policy applies to all personnel of WA Health (employees, contractors, students, volunteers and agency personnel) incorporating the following entities:

- Department of Health
- Metropolitan Health Services
- WA Country Health Service
- Peel Health Service

This policy also applies to external organisations and their personnel who have been granted access to WA Health Information and Communications Technology (ICT) infrastructure and services.

This policy must be read in conjunction with the *Acceptable Use – Computing and Communication Facilities Standard,* which governs the use of ICT by WA Health personnel. This and other policies and standards associated with information security are available at the Health Information Network (HIN) Strategy website.

Controls associated with information security are outlined in the following Australian standards

- *AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems – Requirements.*
- *AS/NZS ISO/IEC 27002:2006 Information Technology - Code of Practice for Information Security Management; and*
- *AS/NZ ISO/IEC 27799:2011 Information Security Management in Health Using ISO/IEC 27002; and*
- *ISO/IEC 27005:2011: Information technology - Security Techniques - Information Security Risk Management.*

3. POLICY

3.1 Access to, use or disclosure of information held by WA Health must be lawful and managed on a 'need to know' basis for legitimate WA Health business requirements.

3.2 The following information security objectives are to be achieved for all WA Health information irrespective of the media on which it is stored or the means of access, use, transmission or preservation:

- **confidentiality - information is only available to authorised users for approved purposes;**
- **integrity – information is complete, accurate and valid and only authorised changes are made to it;**
- **availability – information is available as and when required for authorised purposes;**
- **privacy – collection, use and disclosure of person-identifiable information is managed in accordance with national privacy principles;**
- **authentication – controls are in place to validate the identity of an entity accessing or providing information or undertaking a transaction; and**
- **non-repudiation – controls are in place to assure that the origin and delivery of an information transaction, and the involvement of the parties in the transaction cannot be denied.**

3.3 Users of WA Health information must comply with relevant statutes, directives, policies and contractual obligations governing the information lifecycle. While the Commonwealth Privacy Act 1988 does not apply to the WA Public Sector, the WA Public Sector Commission requires that management of information must be consistent with *National Privacy Principles* in the Act.

The *Operational Circular OP 2050/06 - Patient Confidentiality and Divulging Patient Information to Third Parties* details the general circumstances in which confidential patient information may be disclosed to third parties under the common law.

The *Practice Code for the Use of Personal Health Information* contains the guidelines that must be followed in the design and conduct of all projects using personal health information held in data collections by Department of Health WA.
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*

3.4 Information maintained by and for WA Health must:

- **be managed in accordance with the *Information Lifecycle Management Policy*;**
- **have designated stewards and custodians, who have responsibilities for the protection of information assets and are accountable for those responsibilities in accordance with the WA Health *Data Stewardship and Custodianship Policy*;**
- **be subject to security controls to allow access by authenticated and authorised personnel only;**
- **must be controlled in accordance with WA Health *Information Access and Disclosure Policy***
- **be classified, protected and managed according to the WA Health *Information Classification Policy*;**
- **be protected from theft and accidental or intentional damage, corruption, destruction, disclosure or loss;**
- **be maintained in accordance with the *State Records Act 2000* and the *WA Health Record Keeping Plan* with appropriate retention and disposal schedules and methods;**
- **be preserved over the required retention period and its availability maintained over successive technology or environmental changes;**
- **be subject to backup and recovery in accordance with business continuity plans;**
- **be subject to appropriate levels of audit logs of access, addition, alteration, or deletion; and these audit logs must be regularly monitored to identify anomalous use. Audit logs must also be subject to security controls. Audit logging must also cover administrator and operator access;**
- **be monitored for security incidents, which if detected are then managed according to incident response and forensic plans;**
- **be protected from cyber threats through appropriate technical and behavioural measures;**
- **be protected from exposure and threats from inappropriate use of social media;**
- **be housed in facilities, including data centres and off-site storage, that have appropriate physical security and environmental controls;**
- **be managed by organisations and personnel who are subject to enduring information security requirements either under legislation, binding contracts or agreements, and where applicable have been subject to the *WA Health Criminal Record Screening Policy* requirements;**
- **if shared with third parties, be subject to enduring information security agreements which include provision for external audits;**

- **be stored, transported or transmitted on secure and reliable infrastructure;**
- **be managed on reliable, well-maintained infrastructure for required availability and response times;**
- **be subject to integrity controls and checks;**
- **be lawfully collected, acquired, used, disclosed and disposed, including compliance with intellectual property rights;**
- **be disposed of in a secure manner appropriate with the sensitivity of the information;**
- **be removed from equipment or media that are to be disposed of using appropriate data sanitisation methods, or are to be sent outside WA Health premises for repair or maintenance; and**
- **be accounted for during personnel exiting procedures.**

3.5 HIN ICT risk assessments must include security vulnerability and threat assessments.

3.6 ICT infrastructure, e.g. servers, storage and network, must be protected from unauthorised access, and where possible access must be logged for audit purposes.

3.7 WA Health information security incident response plan and procedures must be maintained and communicated by the Health Information Network.

3.8 WA Health electronic transactions and events must time-stamped, based on system time synchronisation to a reliable high precision reference clock.

3.9 WA Health must maintain a governance framework for information security with enterprise-wide oversight by senior management.

3.10 WA Health personnel must be:

- **regularly educated on their information security roles and responsibilities.**
- **educated to recognise cyber and social engineering threats and the security responses required of them, including the reporting of incidents.**
- **made aware of the information security risks and threats in the use of social media, including that of identity theft, and**
- **educated on the security incident management procedures and reporting of events.**

3.11 Information security roles and responsibilities must be clearly defined for enterprise and local organisational levels and assigned to WA.

Health personnel with the authority to fulfil the defined responsibilities. These roles and responsibilities must be communicated to WA Health personnel.

3.12 ICT roles and duties, and associated access rights must be sufficiently segregated to minimise risk.

3.13 ICT infrastructure must support required availability through measures such as redundancy, failover, fault tolerant approaches and capacity management.

4. POLICY DETAILS

4.1 Information Security Responsibilities

The Health Information Network is responsible for providing a secure ICT environment to support WA Health personnel in protecting electronic WA Health information. HIN is responsible for establishing information security roles, responsibilities and procedures and communicating these to users.

WA Health personnel are responsible and accountable for their use of information and where appropriate the management of security controls for the storage, transmission, access, transfer, disclosure and disposal of information under their control. These responsibilities include compliance with legislative and policy requirements.

Individuals must not divulge or share their WA Health passwords with anyone – including helpdesk technicians, co-workers, managers, friends or family members.

Personnel who breach WA Health security policies may be subject to disciplinary action and other remedies available through legislative provision such as the *Public Sector Management Act 1994* and the *Criminal Code Act 1913*. Unauthorised access to and disclosure of confidential information is misconduct pursuant to the *Corruption and Crime Commission (CCC) Act 2003* and suspected cases may be reported to the CCC. Refer to the *WA Health Misconduct and Discipline Policy*

4.2 Security Incident Reporting and Escalation

Personnel who are aware of an information security breach or incident must report the event to the WA Health ICT Service Desk. The Service Desk will record and refer the incident to HIN ICT Security.

4.3 Information In Transit

Information that is in transit must be subject to appropriate security controls. Unsecured confidential or commercially sensitive information must not be held on mobile or remote devices, transmitted over the internet, public switched telecommunications networks, or unsecured wireless networks, unless the

transmission of this information is protected by appropriate encryption and authentication processes (e.g. password protection, public key infrastructure, secure file transfer, encrypted drives, and secure USB devices).

4.4 Mobile Devices / Removable Media / Remote Access Devices

WA Health information (including photos of patients' wounds or other digital images, etc.) held on mobile phone and computing devices (such as phones, notebooks, tablets, personal digital assistants etc.), portable storage and removable media (including external drives, USB devices, flash cards, cameras and media players etc.) and remote access devices must be considered to be information-in-transit and subject to stringent security controls.

Use of mobile phone and computing devices must comply with the relevant WA Health policies available on the Health Information Network Strategy website:

- *Mobile Computing Devices Policy and Guidelines*
- *Mobile Telephones Policy and Guidelines*

Use of removable media is covered in the *Managed Infrastructure Standard S10.7– Media Handling.*

Transferring sensitive data between organisations via USB devices is not encouraged and personnel are requested to use alternative options listed on the HIN Intranet page under HIN Operations.

Only WA Health registered USB devices should be connected to your work computer. These encrypted devices are safe to use and display the Department of Health logo on the side of the unit for easy identification.

4.5 Desktop storage

Desktop computer storage drives must not be used as primary or permanent storage for corporate data. Where desktop drives are used for temporary storage purposes, sensitive or critical data must be subject to stringent security controls.

4.6 Output Devices

Printers, facsimile machines and other devices, where sensitive information is to be output, must be subject to security controls. These controls can include location in secure areas, pins/password controls and oversight by personnel.

4.7 Data Centres

Whether data centres and services are operated directly by WA Health or managed through contracted arrangements, WA Health has a responsibility to ensure data protection measures are in place. Contracted arrangements must specify the responsibilities of all parties in protecting WA Health's information.

To securely support health services which operate 24 hours a day for each day of the year, and due to the criticality, volatility, sensitivity and volume of patient data, WA Health requires its information to be hosted, transacted, processed and supported in data centres connected by high bandwidth, low latency communications, supported by reliable infrastructure and utilities.

WA Health prefers that its operations and highly sensitive data be physically located in WA; this requires that its data centres and the off-site storage services are physically located in WA.

4.8 Support Personnel

WA Health prefers that ICT operations support for its patient, clinical and other information systems processing sensitive information, and service-desk support (including remote support of workstations), are provided by personnel who are physically located in WA and who are subject to Australian and Western Australian laws and policies.

WA Health recognises that some non-routine problem resolution, upgrade or maintenance services may be provided remotely by personnel located in jurisdictions external to Western Australia; however such services must be subject to strict security controls and monitoring by WA Health personnel, and network access permitted only under formal access arrangements.

ICT personnel and organisations providing services to WA Health who are not covered by WA public sector confidentiality obligations must be required to sign confidentiality agreements. ICT personnel must be required to provide evidence of security clearances in accordance with the WA Health *Criminal Record Screening Policy and Guidelines*.

4.9 Contracting and External Sourcing

Where third party organisations are contracted to provide services that include information and communications technology services, the contracts must contain appropriate measures for the protection of the information and infrastructure, including criminal record screening of contractors' personnel.

Legal advice must be sought before arrangements are entered into that may involve transborder storage or flow of WA Health information.

The HIN *Network Access Standard* describes available connection methods to the WA Health network. It is supported by formal agreements for network access by external parties.

4.10 Cloud Computing

Cloud computing covers a multitude of possible arrangements from formal hosting contracts, to use of document/data storage and collaborative facilities such as Google Docs, Dropbox, Amazon S3, etc. Many of these cloud computing facilities are trans-border services and introduce complex legal

issues in the event of security breaches.

The Health Information Network routinely blocks access to such sites. Personnel who require access to blocked sites need to seek approval from the Corporate Governance Directorate.

WA Health information must not be stored on external cloud computing services without agreements for the management of the information in accordance with government policy and legislative requirements such as *Freedom of Information Act 1992* and *State Records Act 2000*, and for the protection of the information in accordance with WA Government and WA Health confidentiality and privacy requirements. Agreements with Cloud service providers need to ensure that:

- WA Health has ownership of WA Health information;
- WA Health knows the site(s) of the storage;
- retention and disposal of information is in accordance to WA Health Record Keeping Plan and the State Records Act; and
- if personal information is also stored, security arrangements are in place to protect misuse of the information.

An alternative to commercial cloud collaborative services is the govdex service hosted and provided by the Commonwealth Department of Finance and Deregulation. Potential users should review the govdex Terms and Conditions to determine suitability of the service for their requirements.

4.11 Cyber Threats

WA Health has in place boundary controls that include but not limited to monitored 24/7 Intrusion Detection and Prevention Services, Firewalls and a centrally managed anti-malware service.

HIN routinely blocks access to sites that are considered security risks.

Devices connecting to the WA Health network must comply with current anti-malware levels and be scanned regularly. This includes any externally owned devices connected to the WA Health network for specific purposes (e.g. AGFA imaging workstations, or paging servers).

Security patches provided by operating systems and application software vendors must be applied to guard against cyber threats (subject to appropriate change management procedures).

User Identification (‘he’ numbers) assigned to WA Health personnel and associated passwords must not be used as credentials for registration at non WA Health information systems, websites or email services.

WA Health personnel must not respond to any request whether via email or other communications to divulge their WA Health password or similar security credentials. Similarly for the protection of their own personal assets they must be vigilant against cyber social engineering attempts to make them disclose personal information such as banking details.

4.12 Social Media

WA Health personnel must ensure that their use of social media is safe, and does not introduce risks to WA Health's information and infrastructure through inappropriate exposure or disclosure of information, or through unsafe practices. The WA Public Sector Commission has released *Social Media Guidelines for the WA Public Sector* and WA Health has released a *Policy on Use of Social Media*. The Health Information Network has blocked access to some social media sites. Personnel who require access to such sites need to seek the approval of the Corporate Governance Directorate.

4.13 Security Measures

System documentation, and details of security control measures and their implementation, use and maintenance shall also be subject to appropriate protective measures. Security controls shall be tested on a periodic basis to ensure their continued effectiveness.

4.14 Personnel Exit Procedures

Electronic information, including electronic files, emails or address lists, created and received by or on behalf of WA Health are government records and do not belong to the individual.

As with other government assets, exit procedures for any individual completing their employment or contract with WA Health should include checks that the individual has returned and accounted for all government information and ICT assets in their possession, including any security tokens. This includes all information and equipment assigned to the individual for teleworking arrangements.

The unauthorised removal from WA Health custody by exiting personnel of originals or reproductions of government records including emails is contrary to WA Health records management policy. Government information that is not public information must be removed from any privately owned device that has been authorised for WA Health use.

Personnel exit procedures must include the de-provisioning of any access that the person may have had to all WA Health networks, infrastructure and applications, including the resetting of shared access credentials.

4.15 Disposal of ICT Equipment and Data Storage Media

ICT equipment and media used for storing WA Health information must be sanitised of data and disposed of according to the WA Health *Disposal of ICT Equipment Policy*.

4.16 Official Information and Public Comment

WA Health personnel are not permitted to use official information obtained through the course of their employment to provide public comment or communicate in writing or online without the express authorisation of their Chief Executive Officer. Refer to the *Policy on Use of Official Information and Public Comment* for further information.

5. IMPLEMENTATION

WA Health ICT governance will include oversight of an information security management system with defined information security roles and responsibilities and security risk management, including incident response plans.

It is the responsibility of all WA Health personnel to observe and comply with the Information Security Policy and associated guidelines, standards and procedures.

Induction procedures for WA Health personnel must include an overview of user responsibilities and accountabilities for information security.

Information security responsibilities must be communicated to all personnel in WA Health in a clear and concise fashion. It must also be made clear that non-compliance with these responsibilities may result in consequences ranging from disciplinary action to prosecution.

WA Health entities must ensure that employees handling personal and confidential data have signed confidentiality agreements that clearly spell out their information security responsibilities, and the consequences of breaching confidentiality.

6. BACKGROUND

The WA Public Sector Commission supports an approach to information security in WA Government agencies that is based on the identification and assessment of risks, and the implementation of controls and procedures appropriate to the level of risk and the business needs of the organisation.

WA Health handles very large volumes of information. In addition to the normal commercial and personal information collected, held or used by most government agencies, WA Health maintains personal health information that is generally considered private and sometimes sensitive by the people to which it relates. A key outcome of information security is to ensure the confidence and trust of patients in the way WA Health manages and handles confidential, private and sensitive

information, while ensuring that it is available to those who have a legitimate need or right to know.

Information in WA Health is held in many forms such as medical records, reports, personnel records, paper files, computerised databases and documents. It may be transmitted in many ways including by hand, courier and electronically using dedicated and shared communications lines. Information may be transmitted through systems controlled by WA Health and systems controlled by external parties. The principles underlying the need for information security apply to all information irrespective of the media on which it is held.

The ability to copy, share, search, manipulate and combine data and have the same information accessed concurrently by many people in computerised systems imposes the need for additional controls over information access in such systems. The involvement of personnel, equipment, software, and facilities, which are often not under the direct control of information owners, necessitates the implementation of additional control measures and mechanisms over the operation and use of information technology based systems. On the other hand, the use of information technology in itself enables the use of more sophisticated and thorough controls over the confidentiality, integrity and availability of information than is generally available for information that is not computerised.

7. RELEVANT LEGISLATION AND GOVERNMENT POLICIES

(WA Acts are available at the State Law Publisher website, Commonwealth Acts are available at the Australian Government ComLaw website)

- Criminal Code Act 1913 (WA)
- Corruption and Crime Commission (CCC) Act 2003 (WA)
- Freedom of Information Act 1992 (WA)
- Healthcare Identifiers Act 2010 (C'wlth)
- Privacy Act 1988 (C'wlth)
  - National Privacy Principles
  - Information Sheet No. 8-2001: Contractors
  - Information Sheet No 14-2001: Privacy Obligations for Commonwealth Contracts
- Public Sector Commission Circulars
  - 2009-29 - Policy Framework and Standard for Information Sharing Between Government Agencies
  - 2011-04 - Social Media Guidelines for the WA Public Sector
- Public Sector Management Act 1994 (WA)
- State Records Act 2000 (WA),

8. ASSOCIATED DEPARTMENT OF HEALTH POLICIES, STANDARDS AND GUIDELINES

WA Health ICT policies are available on the Health Information Network Strategy intranet site:

- Acceptable Use – Computing and Communication Facilities Standard
- Computer Virus Protection and Security Software Standard
- Disposal of ICT Equipment Policy
- Logon Standard
- Mobile Computing Devices Policy and Guidelines
- Mobile Telephone Policy and Guidelines
- Network Access Standard
- Sharing Information for Continuity of Health Care Policy

See also Managed Infrastructure Standards available on the Health Information Network Infrastructure intranet site:

- Managed Infrastructure Standard – Media Handling.

Other related WA Health policies and plans are

- Operational Directive OD 0275/10 - Criminal Record Screening Policy and Guidelines
- Operational Directive OD 0321/11 - Data Stewardship and Custodianship Policy
- Operational Directive OD 0304/10 - Information Classification Policy
  Operational Directive OD 0360/12 - Information Access and Disclosure Policy
- Operational Directive OD 0371/12 - Information Lifecycle Management Policy
- Operational Directive OD 0323/11 – WA Health Misconduct and Discipline Policy
- Operational Circular OP 2050/06 - Patient Confidentiality and Divulging Patient Information to Third Parties
- Operational Directive OD 0327/11 - Policy on Use of Official Information and Public Comment
- Operational Directive OD 0326/11 - Policy on use of Social Media
- Practice Code for the Use of Personal Health Information
- WA Health Record Keeping Plan

9. NATIONAL & INTERNATIONAL STANDARDS / SPECIFICATIONS

- AS/NZS ISO/IEC 27001:2006 Information Technology – Security Techniques – Information Security Management Systems - Requirements
- AS/NZS ISO/IEC 27002:2006 Information Technology - Code of Practice for Information Security Management
- AS ISO 27799:2011: Information Security Management in Health Using ISO/IEC 27002

- ISO/IEC 27005:2011: Information technology - Security techniques - Information Security Risk Management
- HB 174:2003: Information Security management — Implementation Guide for the Health Sector
- HB 231:2004: Information Security Risk Management Guidelines

10. REFERENCES

Australian Government Protective Security Policy Framework

Australian Government Information Security Manual (previously ACSI 33);

Office of the Australian Information Commissioner:

11. DEFINITIONS

WA Health's Information	Anything spoken, overheard, written, stored electronically, copied, transmitted or held intellectually concerning WA Health's general business, information systems, employees, business partners, patients, or customers
Personal Information	Information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

12. VERSION CONTROL

Current Version	**Effective Date:**	**Operational Directive No:**	**SHEF ICT Approved Date:**	**Next Review Date:**
2.0	10 September 2012	0389/12	16 July 2012	September 2015
Responsible Group: Health Information Network - Strategy			**Enquiries Contact** Manager ICT Policy	
Version Notes 2001 Original Version				
2008 September - Amendment 1: – Changed AS/NZS ISO/IEC 27001, 27002:2006 (supersedes AS 17799:2006) – Approved Director Information Policy & Support.				
2012.September V 2.0 – Updated to meet revised Australian Standards and technology and industry changes				