Government of Western Australia
Department of Health

Policy Frameworks
MP 0067/17
Effective from: 27 July 2020

Information Security Policy

1. Purpose

The WA health system depends on effective information security management to protect the confidentiality, integrity and availability of health information and systems. Protecting confidentiality is essential for maintaining the privacy of patients; protecting the integrity of health information is critical for ensuring patient safety; and ensuring the availability of information systems is critical for healthcare delivery.

Appropriate technical, physical and administrative security controls are required to safeguard the WA health system from inappropriate, illegal or accidental misuse, exposure or corruption of data and technology.

This *Information Security Policy* (Policy) outlines the security controls required to be implemented, monitored and reviewed across the WA health system. It aligns to the principles of the Australian Standards for information security management which supports a risk-based approach to information security that is appropriate to sensitivity, risk profile and business need.

The purpose of this Policy is to ensure:

- appropriate information security controls are in place to protect health information and systems from theft, fraud, malicious or accidental damage, and privacy or confidentiality breaches; and
- alignment with Australian Standards for Information Security
    - AS/ISO 27002: 2015, *Information Technology – Security techniques – Code of practice for information security management*
    - AS/ISO 27799: 2011, *Information security management in health using ISO/IEC 27002*.

This Policy is a mandatory requirement under the *Information and Communications Technology Policy Framework* pursuant to section 26(2)(k) of the *Health Services Act 2016*.

This Policy supersedes the *ICT Physical and Environmental Security Policy* (OD 0506/14) and the *Network Access Policy* (OD 0505/14).

2. Applicability

This Policy is binding upon all Health Service Providers, the Department of Health (known hereafter as "the Department") and their staff. In addition, Health Service Providers and the Department must ensure that in contracting with Contracted Health Entities, the entity and any of their personnel accessing the WA health system comply with all relevant

mandatory requirements listed in this Policy. This includes any person working in a permanent, temporary, casual, contracted, termed appointment or honorary capacity.

This Policy also applies to any entities, medical technologies, systems or individuals that access or use the WA health system network. This includes any device that stores or accesses the WA health system information and systems. Devices include (but are not limited to) computers, laptops, mobile devices, USB devices, wearables and all backup systems (physical and on the Internet).

Where a Health Service Provider or the Department has arranged local ICT services (rather than the service provided by Health Support Services (HSS)), they have responsibility for implementing the policy. Local ICT services includes the large structured arrangements (such as at Fiona Stanley Hospital, Perth Children's Hospital and WA Country Health Service) small, localised business units operating their own ICT services and contracted arrangements with external providers.

3. Policy requirements

Implementation of the policy requirements should be done using an appropriate risk-based approach and without impacting service delivery and patient safety. Exceptions to implementation require appropriate approval from an Authorised Officer Tier 3 or above.

To ensure a consistent approach to the management of information communication technology risks, the WA Health *Risk Management Policy* (MP 0006/16) which already applies to Health Service Providers, must also be applied to the identification and management of information security risks. Further, the Department should identify and manage information security risks in accordance with the WA Health *Risk Management Policy* (MP 0006/16) to the extent they are able.

Security risks are to be recorded in the approved risk management system of the relevant Health Service Provider, the Department or Contracted Health Entity. Local ICT security issues are to be reported to the local ICT governance body; enterprise or network security issues must be reported to the local ICT governance body and the HSS ICT Security Working Group.

3.1 Security objectives

In accordance with the WA Government Digital Security Policy the following security objectives apply to the WA health system information and systems:

- **Confidentiality** – the treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission
- **Integrity** – data is protected against unauthorised alteration or destruction and any challenges to health information authenticity are prevented, giving consumers confidence in the way the WA health system protects and handles health information
- **Availability** – authorised users are provided with timely and reliable access to health information and systems for authorised purposes
- **Privacy** – the individual's right or expectation that health information and other identifying information will not be disclosed.

3.2 Information security controls

All Health Service Providers, the Department and Contracted Health Entities must have processes in place to support the following information security controls.

3.2.1 Access control

Access to the WA health system information and information processing facilities must be controlled and limited, in accordance with the following overarching principles:

- **Need-to-Know** and **Need-to-Use** principles: users are only granted access to the information or information processing facilities they need to perform their tasks
- **Principle of Least Privilege**: only the minimum privileges necessary to complete required tasks will be assigned to each user
- **Segregation of Duties (or Separation Principle)**: the granting of roles, duties and associated access rights must be sufficiently segregated to minimise risk and avoid conflict of interest.

3.2.1.1 Passwords and Authentication

All WA health system access accounts must be protected with strong passwords, or other secret authentication information, to validate the identity of an entity accessing, providing information or undertaking a transaction. Strong passwords as defined by industry best practice are to be applied wherever the system allows. Passwords are to remain confidential at all times and be securely stored using encryption.

3.2.1.2 Privileges

Processes for the management and use of allocated privileges must be established that comply with the following standards and requirements:

- privileges assigned to each individual are to be monitored by line managers and data custodians, and modified or revoked upon a change in individual status with the organisation. These privileges are also to be reviewed at regular intervals using a formal process to ensure they are complete, accurate and access is still required
- the network access rights of all staff members are to be removed upon termination of their employment or contract. Staff responsible for managing other staff members must ensure those exiting the organisation have their access immediately revoked, by initiating and approving an HFN-030 Access Request Form prior to exit. Regular reviews of inactive accounts, as an established process, are required
- privileges should be role based rather than individual specific
- individuals requiring highly privileged access (eg system administration / super user access) rights are to be assigned a different user identification (ID) for this purpose, which is separate from their user ID used for regular business activities. Regular business activities should not be performed using highly privileged IDs.

3.2.1.3 Individual access accounts

A formal user registration and termination process must be established to grant access by individuals to the WA health system's information systems that complies with the following:

- approval for access to be provided by authorised officers, consistent with Authorisation Schedules, Policy Frameworks, and relevant local policies
- HSS to assign a WA health system identifier and User Credentials for identification and authentication purposes to each individual that has a business, or other approved need to access the WA health system ICT resources. HSS may enable other entities to assign WA health system identifiers and User Credentials for their staff, consistent with user provisioning requirements set out by HSS

- all internal requests for access to be initiated via the HFN-030 Access Request Form. See section 3.2.1.6 for access by external users
- for non-permanent staff members, user accounts to be set to expire in accordance with the contract expiry date
- all individuals must agree to comply with the WA Health *Acceptable Use of Information and Communications Technology Policy* (MP 0066/17) and a record of this agreement must be maintained
- where access to systems is provided via swipe card technology, individuals must immediately report any lost or stolen system access/swipe cards to ensure access can be de-provisioned immediately.

3.2.1.4 Group / generic logon accounts

Group / generic logon accounts (ie accounts created for more than one individual to use) are not permissible without the documented approval by an Authorised Officer Tier 3 or above. Where approved, the Authorised Officer remains accountable at all times for the access to the information via that group / generic logon account and will ensure:

- procedures are developed to ensure passwords are updated as appropriate, confidentiality is maintained, and usage can be monitored;
- a regular monitoring and audit process is in place;
- a risk assessment is undertaken and mitigation strategies in place to prevent any accidental or intended shared use of application logons, particularly where single sign-on arrangements are enabled for workstations. These strategies may include shorter application timeouts (where possible) and/or stringent guidelines for use;
- procedures are in place for highly privileged or administrator group / generic logon accounts to ensure the account is used for its intended system configuration capabilities only; and
- all accounts are reviewed by the Authorised Officer at regular intervals using a formal risk-based process to ensure they are still required and the appropriate approvals for use exist.

3.2.1.5. Single sign-on arrangements

All Health Service Providers, the Department and Contracted Health Entities must ensure single sign-on access arrangements have controls in place to maintain information security, particularly in relation to any additional risks associated with shared workstations. These may include, but are not limited to, appropriate application timeouts, standards and guidelines for implementation and use, and clear user identifiers/banners.

3.2.1.6. Access by external organisations

All external organisations (e.g. vendors) requiring access to the WA health system information and information systems for project, business or maintenance purposes must submit requests for access to HSS using the following forms:

- HFN-057-Request for Network Access by External Organisations
- HFN-060-Agreement-for-Network-Access

All external remote access accounts including any Virtual Private Network (VPN) arrangements are to be reviewed by the relevant Health Service Provider or the Department at regular intervals using a formal risk-based process to ensure they are complete, accurate and access is still required.

3.2.2 Cyber threats and malware

All WA health system information systems (including third party managed systems attached to the WA Health network) require security controls to be in place to prevent the exploitation of technical vulnerabilities from cyber threats and malware. These should be implemented by Health Service Providers, the Department and Contracted Health Entities as outlined in section 2 Applicability. Cyber security planning, processes and procedures that include detection, prevention, reporting and management of incidents must be implemented. These plans, processes and procedures must contain the elements outlined below:

- intrusion detection and prevention services that are monitored 24 hours a day / 7 days a week and include the ability to conduct audit analysis and system integrity checking
- technical vulnerability scans that have items identified and patched in a timely manner, adequate patch testing and patch testing documentation that is maintained and periodically reviewed
- reporting mechanisms to assess and take remedial action
- systems in place to receive early warnings of alerts, advisories and patches
- where the system allows, mobile devices connecting to the network must be compliant with current anti-malware requirements and scanned regularly
- security patches provided by vendors must be installed in a timely manner to mitigate vulnerabilities and guard against cyber threats. Health Service Providers and the Department must have standard change control processes with outage notification and scheduled windows to apply these patches. In cases where an urgent security patching is required, the standard process must be accelerated and out of band changes arranged with the business
- where a system is unable to be patched and maintained within appropriate security best practice, containment strategies need to be applied to minimise the risk to the remainder of the WA health system. Costs associated with identifying, purchasing and implementing these containment strategies are to be borne by the Health Service Provider, the Department or business unit that requires the retention of the legacy system / service
- border gateway services (also referred to as network firewalls) must be reviewed at regular intervals, in line with a risk-based approach for replacement / or upgrade. Border gateway services must be intrusion tested regularly (see dot point one in this section)
- centrally managed anti-malware service by HSS for HSS-managed systems and applications
- the requirement for WA health system employees and external parties to comply with the *Acceptable Use of Information and Communications Technology Policy* (MP 0066/17).

The Australian Signals Directorate also sets out the top Strategies to Mitigate Targeted Cyber Security Incidents, which are recommended for implementation by Health Service Providers, the Department and Contracted Health Entities wherever possible.

3.2.3 Data encryption

Where possible and practicable, encryption must be used to protect the security of WA health system information at rest and in transit. Specifically,

- **Data at rest**: confidential or health information must not be held on portable storage devices, including mobile phones, unless it is protected by current industry best practices encryption. Passwords must also be securely stored using encryption. Data at

rest in applications and medical devices (e.g databases) must be encrypted where possible.
- **Data in transit**: confidential or health information must not be transmitted over the internet, public switched telecommunications networks, or unsecured wireless networks, unless the transmission of this information is protected by encryption or other approved secure methods (see section 3.2.5).

Examples of controls include the use of public key infrastructure, secure file transfer, encrypted USB and mobile devices and email encryption.

Section 3.2.5 Data storage, transfer and disposal outlines secure USB and secure file transfer solutions available for use in the WA health system.

To maintain the security and integrity of encryption keys, and prevent data loss, an encryption key management process must be developed, implemented and managed by Health Service Providers, the Department or Contracted Health Entities in accordance with section 2 Applicability. This process should cover the management lifecycle of generating, storing, archiving, retrieving, distributing, retiring and destruction of keys.

The use of digital certificates and management of keys for the My Health Record system must be in accordance with the Australian Digital Health Agency and *My Health Record (MHR) Policy* (MP 0094/18).

3.2.4 Data storage, transfer and disposal

The storage, transfer and disposal of health information must be undertaken in accordance with its sensitivity and risk profile (see *Information Management Policy Framework*), and protected in accordance with the security controls listed below.

3.2.4.1 USB devices

Only WA health system approved USB devices are to be connected to the WA health system information and ICT environment in order to protect the WA health system from malicious codes and viruses. These encrypted USB devices are safe to use and display the Department of Health logo on the side of the unit for easy identification. WA health system USB devices can be purchased via an HFN-030 form. The use of non-WA health system USB devices in the WA health system network is prohibited and a breach of security.

3.2.4.2 Data storage

3.2.4.2.1 Storage in data centres

All WA health system information must be hosted, transacted, processed and supported in data centres that are connected by high bandwidth, low latency communications, and supported by reliable infrastructure and utilities. This is due to the criticality, volatility, sensitivity and volume of patient data and will ensure that the information is available 24 hours a day, every day of the year.

Whether data centres and services are operated directly by Health Service Providers, the Department or are managed through contracted arrangements, the relevant contracting entity has a responsibility to ensure appropriate measures are in place to protect the data.

Contracted arrangements must specify the responsibilities of all parties in protecting health information to an appropriate level.

3.2.4.2.2 Storage on workstation computers

Workstation computer hard drives must not be used as primary or permanent storage for health information. Where these hard drives are used for temporary storage purposes, data must be subject to stringent security controls (see section 3.2.10 Physical security). Confidential or personal data should not be stored on workstation hard drives.

3.2.4.2.3 Storage in output devices

Printers, facsimile machines and other devices that output confidential or personal information must be subject to security controls. These controls can include physical location in secure areas, PINs/password controls and/or oversight by personnel.

Printing from systems containing high risk or classified data should not occur without PIN or password controls. Where this is not possible, appropriate physical security measures must be implemented to protect the information. Where output devices store information on internal hard drives these must be destroyed in accordance with Section 3.2.5.4 Disposal of storage media.

3.2.4.2.4 Storage on portable devices

WA health system data should be stored in secured application and database servers housed in the WA health system's ICT facilities as these are the designated primary data storage facilities. Where portable devices are used for the capture or transport of original data, such data must be transferred to a primary storage facility as soon as practicable.

Confidential or personal information (including digital images, downloaded patient data, commercially sensitive information etc) must not be held on portable devices unless the device is protected by approved cryptography (e.g. USB devices or laptops issued by a Health Service Provider or the Department; encrypted mobile phone).

Individuals are responsible for the security of the devices at all times, including:

- the secure storage, backup, transmission, access and disposal of information contained on the devices;
- ensuring they are not left unattended or unsecured at any time;
- all use is appropriate and by authorised employees or contractors only (i.e. not used by friends, family or other non-approved staff).

See also section 3.2.5.1 Storage on USB devices.

3.2.4.3 Data transfer

When information is transmitted outside of the WA health system network (e.g. sent via email, SMS or social media over the internet, public switched telecommunications networks or unsecured wireless networks), it is considered unsecured information in transit. Confidential or health information must not be transmitted through unsecured channels without the use of appropriate cryptography. Transferring personal information may also require specific approvals (see *Information Management Policy Framework*).

Any media containing information must be protected against unauthorised access, misuse or corruption during transportation.

3.2.4.3.1 Data transfer via secure file transfer (MyFX or MyFT)

HSS provides secure file transfer services to enable Health Service Providers and the Department to send and receive patient data electronically and safely via My File eXchange (MyFX) and My File Transfer (MyFT). Both systems provide comprehensive enterprise security of health information that is sent or shared, as data is secured by user authentication upon opening attached information.

My File eXchange (or MyFX) is available for adhoc use, and as an on demand self-registration based service to send and receive large files, sensitive and confidential information both inside and outside of the WA health system network.

My File Transfer (or MyFT) is available to enable regular use, and/or ongoing business process integrated file transfer requirements, to send and receive large files, sensitive and confidential information both inside and outside of the WA health system network. It also can provide collaboration based file sharing services between working groups both internal and external to the WA health system.

Interested staff can apply for MyFT access via the HFN-030 form. Note that a license fee applies to this use.

3.2.4.4 Disposal of storage media

Storage media maintained by or for the WA health system that is no longer required must be disposed of in a secure manner appropriate to the sensitivity of the information.

Data contained in physical media or equipment must be removed using appropriate data sanitisation methods at the time of decommissioning ICT equipment (including mobile phones). The only approved sanitisation and destruction methods are:

- physical destruction of the data storage media once removed from ICT equipment, for example, physically drilling through the hard drives or electronic storage media;
- use of ICT equipment sanitisation and destruction services provided under CUA WAS2016 Waste Disposal and Recycling Services; and
- securely wiping a disk or storage media using software.

Written confirmation that the data has been removed from the storage media must be obtained and retained by the Health Service Provider or the Department.

Note that information that is no longer required must be reviewed by the data owner for any data retention requirements. See the *Information Management Policy Framework* for more details.

3.2.5 Mobile devices and computers

This section includes additional security considerations when using a WA health system-owned versus a privately-owned mobile device or computer.

3.2.5.1 Health Service Provider or Department of Health-owned devices

To ensure the security of mobile devices and protection of health information, the following requirements must be met by mobile devices and computers issued by Health Service Providers or the Department:

- up-to-date virus protection, security software patches and software updates must be installed;

- protection of the information on the device with authentication control;
- installation of remote disabling, erasure or lockout software must be installed; and
- re-allocation, retirement or disposal of mobile devices in line with Section 3.2.5.4 Disposal of storage media.

Individuals are responsible for the security of the mobile devices at all times, including:

- ensuring the secure storage, backup, transmission, access and disposal of information contained on mobile devices;
- removing all information from the device when the device is disposed of, transferred to another person or is to undergo repair. (Refer to the *Information Management Policy Framework* for policy requirements for the disposal of information);
- accepting full responsibility to comply with the *Acceptable Use of Information and Communications Technology Policy* (MP 0066/17), Occupational Safety and Health requirements and relevant law including the Road Traffic Code Regulation 265 (use of mobile phones by the driver of the vehicle); and
- ensuring they are not left in vehicles or in the office unattended. Individuals may be held liable for any negligence resulting in lost, stolen or damaged goods, or delay in reporting. Lost, stolen or damaged mobile devices must be reported to the relevant line manager and HSS as soon as possible. If stolen, a report should be made to WA Police to obtain an official report number for insurance purposes. For devices that are stolen and have remote disabling or erasure software installed, HSS may erase all data on the mobile device, including private data. Health Service Provider or the Department staff using the device for storing private data do so at their own risk.

3.2.5.2 Privately-owned devices

Staff are permitted to use privately-owned devices are permitted for work purposes, subject to the general conditions and requirements listed below:

- individuals are responsible for payment of all costs incurred with the use of a privately-owned device, including the device itself, connection, usage and license costs (except where an industrial award has provisions for reimbursement of mobile telephone costs for employer initiated on-call or contact requirements). These costs include work related use
- if the device is to be connected to the WA health system networks it may need to be loaded with specified software (Mobile Device Management Service) to protect WA health system infrastructure and information. Such software may affect the performance of the device. Note that HSS is not responsible for any adverse impact of the software on the privately-owned device
- should the device be mislaid, lost or stolen, the specified software may provide HSS the capability to lock the device or destroy data held on the device. This will include any private data held on the device
- the user is responsible for the protection of WA health system information (e.g. emails) stored on the private device at all times. This includes:
    - protecting the device with passcode control at a minimum (see section 3.2.1.1 Passwords and Authentication);
    - removing all WA health system information from the device when the device is disposed of, transferred to another person or is to undergo repair;
    - secure transmission of data (see Section 3.2.5 Data Storage, Transfer and Disposal);
    - ensuring current malware protection wherever possible;
    - installing auto-location technology to help locate lost or stolen devices;

- appropriate security in accordance with this Policy for any device used to back up or synchronise with the mobile device (i.e. backups to laptops must be encrypted and laptops also appropriately disposed etc.).

The above conditions and requirements under which the private devices may be used for work purposes may be altered without notice.

3.2.5.2.1 Accessing webmail, via a web browser

WA health system email can be accessed on private devices via the internet using authentication controls. Also referred to as "webmail", any employee or contractor is able to access their webmail without additional approvals. By accessing webmail on their private devices, individuals acknowledge the requirements outlined at Section 3.2.5.2 Privately Owned Devices and must comply with secure storage and transmission requirements at Section 3.2.5 Data Storage, Transfer and Disposal.

3.2.5.2.2 Accessing email on device's email application, via push mail

Push mail is a system that automatically forwards emails as they arrive to a device's email application. The technology is also often used for transferring (pushing) non- email data such as contacts and calendar appointments.

The use of push mail for privately owned mobile telephones for WA health system email and other associated Outlook functions (such as calendaring and contacts) is only possible where:

- prior authorisation for work use has been obtained via an HFN-030 form; and
- the private device supports technology used at HSS to synchronise data with Microsoft Exchange mailboxes (eg Microsoft ActiveSync).

By accessing push mail on their private devices, individuals accept and acknowledge the requirements outlined at Sections 3.2.5.2 Privately Owned Devices and 3.2.5 Data Storage, Transfer and Disposal.

3.2.5.2.3 Accessing the WA health system network (BYOD)

Accessing the WA health system network with a privately-owned device, primarily for accessing health data and applications, is commonly referred to as "Bring Your Own Device" or BYOD. The capability is currently only available at limited sites across the WA health system and the functions available vary from site to site. BYOD does not include accessing WA health information via webmail or secure file transfer.

Where BYOD services are established for that site and available for use, privately- owned mobile devices may connect to the WA health system network where the following are available and applied:

- the appropriate technical capabilities to support BYOD have been established for that site;
- as described above (section 3.2.5.2), a Mobile Device Management Service exists or can be installed on the device to protect WA health system infrastructure and information. Such software may affect the performance of the device. Note that HSS is not responsible for any adverse impact of the software on the privately- owned device;
- the WA health system Wi-Fi is available on site;
- any relevant forms, user agreements and approvals required by the hosting Health Service Provider or the Department and HSS have been obtained. The appropriate

process will depend on the site and the Health Service Provider or Department providing the service. Where the BYOD services are available, the Health Service Provider or the Department must establish an appropriate process in conjunction with HSS (to ensure the integrity of the information security). Users seeking to use their own devices should contact their local ICT service within their Health Service Provider or the Department for advice; and
- an agreement has been signed by the requestor (user) indicating their acknowledgement of the conditions outlined at Section 3.2.5.2 Privately Owned Devices and their compliance with the secure storage and transmission requirements outlined at Section 3.2.5 Data Storage, Transfer and Disposal.

3.2.5.2.4 Remote accessing the WA health system via MyRA

HSS provides remote access capabilities for flexible work arrangements and on call support over a VPN facility called My Remote Access (MyRA). This is available on request using the HFN-030 form. Using MyRA allows WA health system employees to access WA health system information offsite without the need for the information to leave the organisation's computer network.

3.2.5.3 Provision of Guest Internet Services

Providing access to the internet via personal devices for guests or visitors of the site rather than WA health system staff should be assessed against the business objectives and associated costs. Costs associated with provision of internet services by the WA health network to guests will be recovered from Health Service Providers.

The capability is currently only available at limited sites and the functionality and suitability for purpose may vary from site to site. Where guest internet services are available, the Health Service Provider or the Department must establish an appropriate user registration and agreement process in conjunction with HSS (to protect the integrity of the information security).

Where guest internet services are established for that site and available for use, privately-owned mobile devices may connect to the WA health system network under the following conditions:
- appropriate technical capabilities to support guest internet services have been established for that site; the WA health system Wi-Fi is available on site;
- guest/visitor technical support arrangements have been established by the Health Service Provider or the Department (in conjunction with HSS if appropriate) to manage any faults or visitor connection requirements. This includes any amendments to contractual arrangements or agreed Service Level Agreements for this service; and
- any relevant forms, user agreements or registration processes have been required by the hosting Health Service Provider of the Department and HSS have been obtained. The appropriate process will depend on the site and the Health Service Provider or Department providing the service.

3.2.6 Monitoring and logging

Access to the WA health system's networks and resources shall be granted to only those entities and individuals who consent to monitoring. For individuals, this is outlined in the *Acceptance Use of ICT Policy* and agreement must be obtained and documented prior to accessing the WA health system's networks and resources. Based on the risk profile of specific information and information systems, an ongoing program of monitoring and

logging is required to ensure events on designated systems are recorded and evidence of any information security incidents can be generated. The monitoring and logging program for the relevant system or application is to be appropriately managed and governed, with meaningful and readable log information retained. Where relevant, event logs should include the HE number, name, module accessed, details of activity/transaction performed and the activity timestamp.

In addition, information systems containing health information should be provided with facilities for analysing logs and audit trails that allow the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time. These facilities may need to be built if they are not available or are inadequate in procured systems.

Audit logs must be read-only, secure and tamper proof. In particular, system administrator activities must be logged and the logs protected, to maintain accountability for privileged users. Logs should be kept for the appropriate retention period to assist in future audit and access control monitoring. Audit logs must be checked regularly.

Where security incidents are detected, these are to be managed according to Section 3.2.12 Security Incident Management.

WA health system electronic transactions and events must be based on system time synchronisation to a reliable high precision reference clock. The timing of events can play an essential role in processes such as coroner's inquests, investigations in medical malpractice and other judicial proceedings where it is essential to accurately determine a clinical sequence of events.

3.2.7 Network security management

To protect WA health system information and ensure ongoing access to network services, networks must be managed and controlled. Security mechanisms, service levels and management requirements of all network services are to be identified and included in network contract agreements. A "Defence in Depth" approach to WA health system ICT access (such as network access control) is to be used where applicable, based on a risk assessment and cost/benefit analysis.

3.2.8 Personnel security

The requirements listed in this section must be addressed to ensure that staff members engaged by HSPs are aware of their responsibilities in relation to information security and are suitable for the roles they are undertaking.

- individuals and organisations providing services to the WA health system who are not covered by confidentiality obligations under the *Code of Conduct* must be required to sign confidentiality agreements.
- all employees must complete mandatory training to understand their responsibilities in relation to Accountability, Ethical Behaviour, and Records Management
- Health Service Providers and the Department must ensure staff are:
    - regularly educated on their information security roles and responsibilities at orientation and on an on-going basis as required;
    - 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.
- ICT operations support for WA health information systems that process sensitive patient, clinical and other information and service-desk support (including remote support of workstations) should be provided by personnel who are physically located in WA and subject to Australian and Western Australian laws and policies wherever possible. 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, network access under formal access arrangements and ongoing monitoring by staff members employed by an HSP or the Department.
- Exit checks for any individual completing their employment or contract with an HSPs, the Department or Contracted Health Entity must include ensuring the individual has returned and accounted for all government information and ICT assets, including any security tokens and electronic records. This also includes equipment assigned to the individual for teleworking arrangements and all information held in a privately owned device. Personnel exit procedures must include the de-provisioning of any access that the person may have had to all WA health system networks, infrastructure and applications (see HFN-030). Individuals are to acknowledge they do not have possession of any WA health system information.

3.2.9 Physical security

Physical and environmental security of ICT systems, infrastructure, facilities/buildings and network components is necessary to prevent unauthorised physical access, damage and interference to health information. Classified data, as per the *Information Classification Policy* (OD 0537/14), may also require additional physical security requirements.

A risk management approach should be followed to identify and implement physical and environmental security controls. This approach must consider the following:

- **Physical security perimeter** – protect areas that contain sensitive or critical information and ICT facilities (eg. appropriate buildings structure of floor to ceiling walls, fire doors, intruder detection systems, CCTV)
- **Physical entry controls** – secure areas that only allow authorised personnel access (i.e. record of date/time of visitors, authentication mechanisms such as access cards, audit trail, visitors/personnel wear visible identification, third party granted restricted access)
- **Secure offices, rooms and facilities** – physical security of offices, rooms and facilities are incorporated in planning and building
- **Protecting against external and environmental threats** – physical protection and avoidance against natural disasters, malicious attacks or accidents (i.e. planning decisions to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster)
- **Working in secure areas** – procedures for personnel and third party providers on a 'need to know' basis, unsupervised work limited to avoid malicious activities, use of physical locks for vacant areas with review plans in place
- **Delivery and loading areas** – control of access points for delivery and loading areas with isolation where possible to ICT processing facilities (i.e. restriction of personnel, secured external doors, inspection of incoming materials and recorded as per asset management requirements)
- **Equipment position and protection** – consideration of site and protection to reduce environmental threats and hazards or opportunities for unauthorised access (i.e.

position of ICT facilities holding sensitive data to reduce viewing by unauthorised personnel, secure storage facilities, environmental controls such as humidity and temperate are monitored). Equipment should be correctly maintained to ensure its continued availability and integrity

- **Supporting utilities** – ensure equipment from power failures and other disruptions by failures in supporting utilities is protected (emergency lighting and communications available, emergency switches/valves to cut off power, water, gas and other utilities located and working). Management is to be alerted in the event of an issue
- **Unattended equipment** – ensure that equipment not in use is sufficiently protected (i.e. password protected screen saver on computers, log off applications not in use, security controls such as passwords on mobile devices)
- **Clear desk and clear screen policy** – sensitive or critical business information to be locked securely to prevent unauthorised viewing or reproduction of information, computers locked or logged off when unattended. Exceptions for workflow purposes to be approved by an Authorised Officer Tier 3 or above
- **Cabling security** – power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage
- **Off-site assets** – equipment, information or software should not be taken off-site without prior authorisation. When off-site, security should be applied to off-site assets taking into account the different risks of working outside the organisation's premises.

3.2.10 Security continuity management

Information security continuity must be embedded in WA health system business continuity and disaster recovery management processes to ensure the required level of security is maintained during an adverse situation.

In accordance with the Whole of Government ICT Disaster Recovery for Business Continuity Policy, Health Service Providers and the Department must:

- establish a business ICT continuity plan, business ICT disaster recovery plan and an ICT incident response plan, consistent with the standards set in the Insurance Commission of WA RiskCover's Business Continuity Management Guidelines and Risk Management Guidelines. These plans need to detail procedures for managing cyber threats from the internet, social engineering and contain details of how staff should respond to cyber threats under various circumstances. The plan should also contain details for escalation to police, including contact details and who is authorised to file a police report
- in accordance with the risk profile, regularly review, test and update plans to ensure they are contemporary and effective.

Within the WA health system, business continuity management must also be performed in accordance with the *Business Continuity Management* (OD 0595/15).

3.2.10.1 Backup and disaster recovery

The WA health systems disaster recovery plans must include documented backup plans and provision for redundancies where required to ensure ongoing availability of information processing facilities. Disaster recovery information must be classified sensitive and secured appropriately.

To prevent loss of data, backup copies of information, software and system images must be taken and tested regularly in accordance with the risk profile and agreed backup plan.

Backups must be stored in a remote location and subject to regular testing to ensure they are reliable for use in an emergency.

Operational procedures must monitor the execution of backups and address failures of scheduled backups. For critical systems and services, backup arrangements must cover all systems information, applications and data necessary to recover the complete system in the event of a disaster and where appropriate backup data should be encrypted.

3.2.11 Security incident management

An information security incident is any event that results in unauthorised access to data, applications, services, networks and/or devices, through bypassing underlying security mechanisms.

Security incidents may be accidental or intentional, and can include:

- access violations by an individual or software;
- breaches of information integrity or confidentiality;
- corruption or disclosure of health information;
- loss of availability of information systems;
- non-compliances with policies or guidelines;
- breaches of physical security arrangements; and
- uncontrolled system changes.

The WA health system's information systems and physical environments must be monitored for security incidents, which, if detected are then managed according to the Health Service Provider or Department of Health ICT incident response procedures (as relevant). In addition, the procedures listed below must be followed:

- for incidents relating to information systems maintained by HSS, staff must report the event to the HSS ICT Service Desk. The Service Desk will record the incident in accordance with the HSS Incident Management Procedure for reporting and escalation of events, and refer the incident to HSS ICT Security
- where a data breach has occurred, the organisational response must be managed in accordance with the *Information Breach Policy* (MP 0135/20)
- where incidents impact patient safety, personnel must also refer to the WA health system *Clinical Incident Management Policy 2019* (MP 0122/19) and any requirements for informing the subject of care (refer to *WA Open Disclosure Policy Statement*)
- where a major incident has occurred, personnel must refer to the *Public Health Policy Framework* – Disaster Preparedness and Management.

To prepare an effective response to ICT security incidents, any Health Service Provider or Department operating information processing facility must ensure:

- an adequate management structure is identified and in place, with the appropriate authority and experience, to prepare, mitigate and respond to adverse situations;
- incident response staff have the necessary authority and competence to manage the incident and maintain required levels of security;
- documented plans, responses and recovery procedures, detailing how the WA health system will manage and maintain its security to the predetermined level, are developed, approved, maintained and tested in accordance with the risk profile; and
- plans and procedures must be communicated to staff members to ensure all staff are aware of their security incident management procedures and reporting of events.

3.2.12 Software licencing, installation and use

Only authorised and licenced software must be used in the WA health system as unauthorised software may introduce malware or viruses and to ensure security patching/updates are up to date. Usage must be in accordance with specified license or copyright terms and conditions. The acquisition, implementation, transfer and retirement of software, including the reassignment of existing site specific applications from one site to another, must be in accordance with the *Information and Communications Technology (ICT) Governance Policy* (MP 0001/16). The procurement of software licences must be in accordance with the *Procurement and Contract Management Policy* (MP 0003/16).

3.2.13 System acquisition, development and maintenance

Information security requirements should be included as an integral part of the entire information systems development and maintenance lifecycle. This includes:

- integrating information security requirements in the early stages of requirements-gathering and design for new information systems or enhancements to existing information systems;
- protecting information involved in application service transactions to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, message duplication or replay. Additionally, information passing over public networks should be protected from fraudulent activity, contract dispute, unauthorised disclosure and modification;
- adequately protecting system development, test and training environments, with consideration for the sensitivity of the data, access control, monitoring of changes to the environment and code stored therein, and the degree of outsourcing associated with the system development;
- testing security functionality during development. Test data should be selected carefully, protected and controlled;
- prohibiting the use of operational data containing personally identifiable or other confidential information for test purposes;
- implementing formal and structured change control processes to ensure adequate management of changes;
- separating development, testing and operational environments to reduce the risks of unauthorised access or changes to the operational environment;
- addressing information security objectives in project management phases and incorporating security risks in both operational and project risk assessments; and
- supporting required ICT infrastructure availability through measures such as redundancy, failover, fault tolerant approaches and capacity management.

3.2.14 Teleworking and remote access

Teleworking refers to all forms of work outside of the office, including non-traditional work environments, such as those referred to as telecommuting, flexible workplace, remote work and virtual work environments.

Health Service Providers and the Department are responsible for ensuring ICT infrastructure is adequate to support the teleworking functions of their staff and are responsible for funding the ICT requirements for teleworking. Requests for remote access are not automatic and some requests may be declined for reasons of security or infrastructure concerns. HSS can provide advice on ICT requirements and support during normal business hours to configure workstations as required. The requirements listed below also apply.

- appropriate infrastructure must be based on requirements (cost estimates and suitability can be provided by HSS)
- virus protection software must be installed and regularly updated
- security software patches must be applied where applicable
- if using workstations and facilities over the internet to access WA health system services, staff must not use user-id / password caching functions nor store unsecured sensitive material on these devices. Some software such as workstation search engines may also pose security risks in the information that is indexed and stored. Staff must consult with their manager to ensure these risks are understood and addressed
- the ICT infrastructure must be stored in a secure location
- WA health system workstations connected to the WA health system network via dedicated links must not be connected to other networks or the internet by any means other than through the WA health system connection
- reasonable safeguards must be taken to protect equipment and data from theft, loss or damage at the off-worksite location
- data files must be regularly backed-up, preferably to corporate file servers, to avoid loss through equipment failure, damage or theft
- ICT assets supplied by the WA health system are public sector resources and must be managed accordingly. For advice on the management of software assets, refer to the Software Asset Management Unit within the HSS Supply Chain.

3.2.15 Third parties and supplier relationships

Where third party organisations are contracted to provide services that include ICT services for the WA health system, contracts must contain appropriate measures to ensure the protection of health information and infrastructure and adhere to system wide policy and processes. These measures include:

- criminal records screening of Contractors' personnel subject to the *Criminal Record Screening Policy* (OD 0275/10) requirements;
- due diligence and procurement operations as outlined in the *Procurement Policy Framework*;
- an agreed and documented risk management approach to supplier process, product and function with a focus on the complete supply chain;
- seeking legal advice and completing risk assessments before arrangements are entered into that may involve interjurisdictional storage or flow of WA health system information, refer to Section 3.2.2 Cloud Services;
- provision for external audits and governance oversight that addresses privacy and security risks;
- documented agreements for network access by external parties in accordance with the information security requirements that ensure adequate security controls are in place as outlined in this Policy;
- business documents to contain "Commercial in Confidence" wording within the footer template to protect WA health system information/ intellectual property; and
- HFN-060-Agreement-for-Network-Access Forms to be agreed prior to contract award.

4. Compliance monitoring

Health Service Providers, the Department and Contracted Health Entities must develop internal processes to manage and monitor compliance with this Policy.

The System Manager, through HSS, may require certain systems and the WA health system network to log transactions and communications whether private or business related.

The System Manager, through HSS and the Department of Health may also carry out compliance audits to ascertain the level of state-wide compliance with this Policy and may provide updates to Health Service Provider Directors of ICT, Chief Executives of Health Service Providers, the Director General and other relevant persons regarding the findings of compliance monitoring activities.

Although systematic and ongoing surveillance of staff emails and internet access logs will not occur, Health Service Providers, the Department and the System Manager through HSS may monitor or investigate staff use of the WA health system ICT network systems and resources.

This will only occur to confirm compliance with the requirements of this Policy and to investigate possible incidents of breaches of security, unauthorised access or Human Resources matters.

A breach in confidentiality and security may be subject to disciplinary action and other remedies available through legislative provision such as the *Health Services Act 2016*, the *Public Sector Management Act 1994* and the *Criminal Code Act 1913*. Unauthorised access, use and disclosure of confidential data, staff misconduct, including breach of this Policy is misconduct pursuant to the *WA Health Code of Conduct* and suspected cases may be reported to the Government of WA Corruption and Crime Commission.

5. Related documents

The following documents are mandatory pursuant to this Policy:

- N/A

6. Supporting information

The following information is not mandatory but informs and/or supports the implementation of this Policy:

- AS/ISO 27000 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary
- AS/ISO 27001 Information Technology – Security Techniques – Information Security Management Systems - Requirements
- AS/ISO 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls
- AS/ISO 27799-2011 Information Security Management in Health using ISO/IEC 27002
- Australian Signals Directorate – Australian Cyber Security Centre – Strategies to Mitigate Cyber Security Incidents - Essential Eight
- Australian Signals Directorate – Department of Defence – Australian Government Information Security Manual – Controls

7. Definitions

The following definition(s) are relevant to this Policy.

Term	Definition
Authentication	Verification that an entity is who/what it claims to be using a password, biometrics such as a fingerprint, or distinctive behavior such as a gesture pattern on a touchscreen.
Authorisation	Information that defines what operations an entity can perform in the context of a specific application.
Confidentiality	The treatment of information that an individual has disclosed in a relationship of trust and with the expectation that it will not be used or divulged to others in ways that are inconsistent with the understanding of the original disclosure, without permission.
Cloud Computing	Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Infrastructure	Cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics.
Data	The term ‘data’ generally refers to unprocessed information, while the term ‘information’ refers to data that has been processed in such a way as to be meaningful to the person who receives it. In this Policy the terms ‘data’ and ‘information’ have been used interchangeably and should be taken to mean both data and information.
Data Breach	A data breach is an incident in which personal, confidential, sensitive or commercial information is compromised, disclosed, copied, transmitted, accessed, removed, destroyed, stolen or used by unauthorised individuals, whether accidentally or intentionally.
Data Centre	A data centre is a repository that houses computing facilities like servers, routers, switches and firewalls, as well as supporting components like backup equipment, fire suppression facilities and air conditioning. A data centre may be complex (dedicated building) or simple (an area or room that houses only a few servers).
Data Custodian	The person(s) responsible for the day-to-day management of a data collection, as nominated by the Data Steward.

Term	Definition
	Data Custodians assist the Data Steward to protect the privacy, security and confidentiality of information within data collections. Data Custodians also aim to improve the accuracy, usability and accessibility of data within the data collection.
Data At Rest	Data at rest is data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way. Data protection at rest aims to secure inactive data stored on any device or network.
Data In Transit	Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network. Data protection in transit is the protection of this data while it is travelling from network to network or being transferred from a local storage device to a cloud storage device. Effective data protection measures for in transit data are critical as data is often considered less secure while in motion.
Data Integrity	Maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
Data Steward	A person with delegated responsibility from the Director General of the Department of Health to manage a data collection. The Data Steward's primary responsibility is to protect the privacy, security and confidentiality of information within data collections. Data Stewards also approve the conditions for appropriate use and disclosure of information for clearly defined purposes that comply with WA Health's statutory obligations and Information Management Policy Framework
Defence in Depth	Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. Components of defence in depth include antivirus software, firewalls, anti-spyware programs, hierarchical passwords, intrusion detection and biometric verification.
Encryption	Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorised users. This cryptographic method protects sensitive data by encoding and transforming information into unreadable cipher text. This encoded data may only be decrypted or made readable with a key.
Health Information	(As per the definition in the *Health Services Act 2016 (WA)*), means: a. Information, or an opinion, that is also personal information, about: i. the health (at any time) of an individual; or ii. a disability (at any time) of an individual; or iii. an individual's expressed wishes about the future provision of health services to

Term	Definition
	the individual; or iv. a health service provided, or to be provided, to an individual; or b. Other personal information collected to provide, or in providing, a health service.
HFN-030	Computer Access Request Form, used to request access to Health network facilities by Health employees. Applications may have their own request for access form.
HFN-057	Request for Network Access by External Organisations Form.
HFN-060	Agreement for Network Access Form.
Information Security	Practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Need-to-Know	Under the Need-to-Know principle, users are only granted access to the information they need to perform their tasks.
Need-to-Use	Under the Need-to-Use principle, users are only granted access to the information processing facilities (IT equipment, applications, procedures, rooms) they need to perform the task/job/role.
Password	A password is a secret word or string of characters used for authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on passwords as one factor of authentication.
Personal information	(As stated in the *Health Services Act 2016 (WA)*) Has the meaning given in the *Freedom of Information Act 1992 (WA*) in the Glossary clause 1. Means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual, whether living or dead - • whose identity is apparent or can reasonably be ascertained from the information or opinion; or • who can be identified by reference to an identification number or other identifying particular such as a fingerprint, retina print or body sample.
Portable Device	Portable devices, include (but are not limited to): • portable storage and removable media (including external hard drives, USB devices, SD and other memory cards) and • mobile phone and computing devices (such as phones, notebooks, tablets, personal digital assistants, media players and cameras).

Term	Definition
Portable and Attractive Items	Under the WA Health Financial Management Manual, these are defined as items of plant and equipment considered to be high risk of theft or loss and warrant controls over their use and management. They are identified based on their associated relevant risk, including portability, attractiveness, security, and ease of theft or loss.
Principle of Least Privilege	Refers to the concept that all user accounts at all times should run with as few privileges as possible, and also launch applications with as few privileges as possible.
Privileged User Accounts	A user account that has the capability to alter or circumvent system security protections is known as privileged. It can also apply to users who may have only limited privileges, such as software developers, but who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.
Privileges	A privilege is an identified right that a particular user has to a particular system resource, such as a file folder, the use of certain commands, or an amount of storage.
Provisioning	Provisioning refers to the enterprise-wide configuration, deployment and management of multiple types of IT system resources. An organization's IT or HR department oversees the provisioning process, which is applied to monitor user and customer access rights and privacy while ensuring enterprise resource security.
Roles	Roles are groups of operations and/or other roles. Users are granted roles often related to a particular job or job function.
Segregation of Duties (or Separation Principle)	Segregation of Duties is an internal control designed to prevent error and fraud by ensuring that no single person can access, modify or use assets without authorisation or detection. The initiation of an event should be separated from its authorisation.
Security controls	Safeguards or countermeasures to avoid, counteract or minimise security risks relating to personal property, or computer software.
Single Sign-On	Single sign-on is an authentication process that allows a user to access multiple applications with one set of login credentials.
Staff member	As stated in the *Health Services Act 2016 (WA)*), a staff member of a health service provider, means – (a) an employee in the health service provider (b) a person engaged under a contract for services by the health service provider. For the purposes of this Policy, staff member also includes: (a) an employee in the Department of Health (b) a person engaged under a contract for services by the Department of Health.

Term	Definition
Two Factor Authentication	Two-factor authentication requires the use of two of the three authentication factors. These factors are: • something the user knows (e.g., password, PIN, pattern); • something the user has (e.g., ATM card, smart card, mobile phone); and • something the user is (e.g., biometric characteristic, such as a fingerprint).

8. Policy contact

Enquiries relating to this Policy may be directed to:

Title: Director, Support Services Strategy and Governance

Directorate: Governance and System Support

Email: ICTStrategy&Governance@health.wa.gov.au

9. Document control

Version	Effective from	Effective to	Amendment(s)
MP 0067/17	13 September 2017	20 September 2017	Original version
MP 0067/17 v.1.1	20 September 2017	15 November 2017	Minor Amendment
MP 0067/17 v.2.1	15 November 2017	09 August 2018	Major Amendment
MP 0067/17 v 2.2	09 August 2018	29 May 2019	Minor Amendment
MP 0067/17 v.2.3	29 May 2019	27 July 2020	Minor Amendment
MP 0067/17 v.3.0	27 July 2020	Current	Major Amendment details summarised below
• Policy transitioned to the current Policy template. • Section 3.2.2 Cloud Services has been removed. Policy requirements relating to Cloud Services are now available in MP 0140/20 *Cloud Policy*. • References to Mandatory Policy and Operational Directive document numbers, names, Policy Frameworks and corresponding hyperlinks have been updated throughout for currency. • Descriptive and hyperlink text to internal and external websites updated at section 3.2.2, 3.2.10, 3.2.14 and 6.0. • Supporting information documents *Advice on Managing the Recordkeeping Risks Associated With Cloud Computing* and *A Guide to Implementing Cloud Services* have been removed.			

10. Approval

Approval by	Dr David Russell-Weisz, Director General, Department of Health
Approval date	28 August 2017

This document can be made available in alternative formats on request for a person with a disability.