Electronic Information Security

Summary All users of NSW Health information systems and assets have the responsibility to uphold confidentiality and protect information entrusted to them. Information security measures and controls must be developed and implemented to ensure privacy of information is preserved, confidentiality of information is protected, integrity of information is maintained, and availability of information is assured.

Document type Policy Directive

Document number PD2020_046

Publication date 09 December 2020

Author branch eHealth & ICT Strategy Branch

Branch contact (02) 8644 2213

Replaces PD2013_033

Review date 09 December 2023

Policy manual Health Records and Information Manual for Community Health Facilities

File number HS19/23325

Status Active

Functional group Clinical/Patient Services - Records, Statewide and selected specialty services
Corporate Administration - Asset Management, Governance, Records
Personnel/Workforce - Conduct and ethics, Security

Applies to Ministry of Health, Public Health Units, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, Affiliated Health Organisations, NSW Health Pathology, Public Health System Support Division, Cancer Institute, Government Medical Officers, Community Health Centres, NSW Ambulance Service, Dental Schools and Clinics, Public Hospitals, Environmental Health Officers of Local Councils, Private Hospitals and day Procedure Centres

Distributed to Ministry of Health, Public Health System, Government Medical Officers, NSW Ambulance Service, Environmental Health Officers of Local Councils, Private Hospitals and Day Procedure Centres

Audience All Staff of NSW Health

Secretary, NSW Health

ELECTRONIC INFORMATION SECURITY

POLICY STATEMENT

All NSW Health Organisations must have appropriate systems and processes in place to adequately and appropriately protect their information systems and assets. This includes the fundamental responsibility to protect information from inappropriate, illegal or accidental misuse, modification, loss or release.

This policy applies to all users of NSW Health information systems and assets, including, but not limited to, employees, contractors, service providers and third parties, and all NSW Health information systems and assets, regardless of the media or location where information is stored, and the technology used to process the information.

SUMMARY OF POLICY REQUIREMENTS

All users of NSW Health information systems and assets have the responsibility to uphold confidentiality and protect information entrusted to them.

Information security measures and controls must be developed and implemented to ensure privacy of information is preserved, confidentiality of information is protected, integrity of information is maintained, and availability of information is assured.

NSW Health Organisations must identify and implement the appropriate scope of an Information Security Management System (ISMS) or Cyber Security Management System (CSMS) that is compliant with the relevant recognised standards.

A risk-based approach must be adopted to identify and prioritise information systems and assets security risks, ensure proper security measures are implemented and mitigate security risks to an acceptable level. These measures may be preventative, detective, responsive or recovery in nature.

A continual improvement process must be adopted to respond to, monitor, review and improve the effectiveness and efficiency of information security measures and controls in a changing environment.

NSW Health Organisations must ensure a consistent and effective approach to the management and where relevant, the escalation of information security incidents.

REVISION HISTORY

Version	Approved by	Amendment notes
December-2020 (PD2020_046)	Secretary, NSW Health	Electronic Information Security Policy has been updated in line with the NSW Cyber Security Policy Version 3 and the NSW Government Information Classification, Labelling and Handling Guidelines Version 2.
October- 2013 (PD2013_033)	Deputy Director General, Governance Workforce and Corporate	Electronic Information Security Policy v3.0 PD2008_052 has been updated in line with Premiers Memorandum M2012-15
PD2008_052	Director General	Electronic Information Security Policy Version 2.

PD2005_314	Director General	Initial Document

ATTACHMENTS

1. Electronic Information Security: Procedures

CONTENTS

1 BACKGROUND 1
1.1 About this document 1
1.2 Key definitions 2
1.3 Legal and legislative framework 2
2 PROTECTION OF INFORMATION SYSTEMS AND ASSETS 3
2.1 Governance 3
2.2 Risk methodology 3
2.2.1 Enterprise Risk Management Framework 3
2.2.2 Risk assessment 4
2.2.3 NSW Health Risk matrix 4
2.2.4 Risk treatment 4
2.2.5 Selection and implementation of security measures 5
2.2.6 Risk monitoring and review 5
2.3 Allocation of resources and training 5
2.4 Performance evaluation 5
2.5 Continual improvement 6
3 INFORMATION SECURITY INCIDENT RESPONSE PLAN 6
3.1 Preparation 6
3.2 Detection and analysis 7
3.3 Containment, eradication, and recovery 7
3.4 Post-Incident Review 7
4 ROLES AND RESPONSIBILITIES 7
4.1 Secretary, NSW Health 7
4.2 Chief Executives 7
4.3 Chief Information Officer, NSW Health 8
4.4 Director Information Security Services, eHealth NSW 8
4.5 Data governance 8
4.6 System administrators 9
4.7 IT technical and support staff 10
4.8 Records and Information Managers 10
4.9 Users 10
4.10 Third party businesses and organisations, consumers and other agencies 10
4.11 Auditor 10
5 RELATED DOCUMENTS 11
5.1 NSW Health policy directives and guidelines 11
5.2 Relevant legislation – NSW 11
5.3 Relevant legislation - Commonwealth 11

5.4 NSW Government policies and directives 12
5.5 Standards 12

1 BACKGROUND

Any persons having access to NSW Health information have a responsibility to maintain the security and confidentiality of critical and sensitive information, including personal and health information.

NSW Health is committed to the provision of appropriate levels of security across all information systems and assets.

Confidentiality, Integrity and Availability are the security objectives that must be applied to NSW Health Organisations' information systems and assets. These objectives will uphold authorised restrictions on access to, and the use and disclosure of, information, to ensure data is protected against unauthorised alteration or destruction and to ensure authorised users are provided with timely and reliable access to information systems and assets.

NSW Health Organisations are required to assure the privacy of information systems and assets that include records containing personal and personal health information about employees and members of the public. This will uphold the individual's expectation and legal right that personal, health and any other identifying information will not be unlawfully disclosed.

Implementation of information security controls to mitigate the risks to sensitive information must be based on a risk management approach to ensure suitable and appropriate information protection.

All information must be classified in accordance with the NSW Government Information Classification, Labelling and Handling Guidelines. The guideline outlines how NSW Government agencies, such as NSW Health, must securely share, handle and protect information according to its sensitivity. Information which needs increased protection is to be either security classified and identified by a protective marking or assigned a Dissemination Limiting Marker (DLM). For NSW Health Organisations, information that has been classified and labelled using any of the six 'OFFICIAL: Sensitive' NSW DLMs or above, must be securely managed to ensure privacy and confidentiality is preserved. This includes the DLMs 'OFFICIAL: Sensitive – Health information' and 'OFFICIAL: Sensitive – Personal'.

The release of information must comply with NSW and Commonwealth legislation and relevant NSW Health policies.

1.1 About this document

This document establishes the provision of appropriate levels of security across all NSW Health Organisations' information systems and assets. It supports the governance of information security and dictates the principles to manage information security.

The security requirements in this document apply to all NSW Health information systems and assets regardless of the media storage location and the technology used to process the information. All security requirements are designed to be technology neutral. The requirements focus is on the fundamental objectives and measures to protect information.

1.2 Key definitions

Availability

Ensuring timely and reliable access to and use of information.

Confidentiality

Handling of information to ensure that it will not be disclosed in ways that are inconsistent with authorised use and its original purpose.

Cyber Security

Cyber Security is the prevention of damage to, unauthorised use of, exploitation of, and - if needed - the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems.

Electronic information

Electronic information is information that is electronically created, processed, held, maintained and transmitted by NSW Health organisations. It also refers to information held electronically for or on behalf of other government agencies or private entities.

Information systems and assets

Refers to any information or communication infrastructure used by NSW Health Organisations and all personnel that work with it. This includes computer hardware and software, to create, process, hold, maintain or transmit electronic information.

Integrity

To protect information against unauthorised alteration or destruction and prevent successful challenges to its authenticity.

Personal health information

Personal health information is personal information or an opinion which concerns an individual's health, medical history or past or future medical treatment. It also includes other personal information collected in the course of providing a health service or information collected in relation to donation of human tissue.

Personal information

Personal information is information or an opinion (including information or an opinion forming part of a database and whether it is recorded in a material form) about an individual whose identity is apparent or can be reasonably ascertained from the information or opinion.

1.3 Legal and legislative framework

NSW Health Organisations that hold records containing either personal information or personal health information must meet the requirements of the:

1. *Health Records and Information Privacy Act 2002* (NSW); and
2. *Privacy and Personal Information Protection Act 1998* (NSW).

2 PROTECTION OF INFORMATION SYSTEMS AND ASSETS

To safeguard information systems and assets, NSW Health Organisations must have an Information Security Management System (ISMS) or Cyber Security Management System (CSMS) that is compliant with recognised standards and implement the relevant controls based on the organisation's requirements and risk tolerance.

Each organisation's security management system must include the following components:

1. Governance;
2. Risk Management;
3. Allocation of Resources and Training;
4. Evaluation; and
5. Continuous Improvement.

2.1 Governance

NSW Health organisations must have an executive-level governance committee accountable for the effective and efficient management of information security risks, associated plans and implementation of controls.

NSW Health organisations must implement security controls locally according to their needs.

2.2 Risk methodology

NSW Health organisations must use a structured approach to information security risk management, consistent with approaches for assessing and treating all types of risk, at all levels and for all activities within NSW Health.

Information security risk management involves identifying the types of risk exposure within NSW Health, measuring those potential risks and proposing means to mitigate them. While it is impossible to remove all risk, it is important to understand the risks and manage and identify the level of risk NSW Health Organisations are willing to accept in the overall context of effective operation and service provision.

2.2.1 Enterprise Risk Management Framework

NSW Health Organisations must assess and manage information security risks in line with the *NSW Health Enterprise-wide Risk Management Policy and Framework (PD2015_043).*

This framework provides a structure for a consistent risk management approach and for embedding risk management across all operations.

The risk management process includes the following steps:

1. Communication and Consultation;
2. Establish the context;

3. Risk Identification;
4. Risk Analysis;
5. Risk Evaluation;
6. Risk Treatment; and
7. Risk Monitoring, Review and Governance.

2.2.2 Risk assessment

Risk identification, analysis and evaluation are taken together and described as 'risk assessment'. Information security risk assessments are performed to allow NSW Health Organisations to assess, identify and modify their overall security. This process is required to obtain management's commitment to allocate resources and implement the appropriate security controls. All risk assessments must conform to the NSW Health Risk Matrix tool in terms of the relationship between likelihood and consequence.

2.2.3 NSW Health Risk matrix

The NSW Health Risk Matrix provides a tool to apply a severity rating to each risk, by assessing the potential consequence of the risk and its likelihood of occurring. The NSW Health Risk Matrix is required to be used for assessment and management of information security risks, development of risk registers and reporting of risks.

2.2.4 Risk treatment

Information security is a combination of preventive, detective, responsive and recovery security measures. Preventive measures avoid or deter the occurrence of an undesirable event. Detective measures identify the occurrence of an undesirable event. Responsive measures refer to coordinated actions to contain damage when an undesirable event (or incident) occurs. Recovery measures are for restoring the confidentiality, integrity and availability of information systems to their expected state.

Once the risks have been identified, analysed and evaluated; treatments are considered. Risk treatment involves selecting one or more options for addressing the identified information security risk(s) and implementing and managing those options. Risk treatment options include:

1. Risk Management / Reduction - The level of risk is to be reduced through the implementation of some or all recommendations made from the risk assessment. Appropriate and justified controls should be selected to meet the risk acceptance criteria as well as legal, regulatory and contractual requirements. When selecting controls, NSW Health Organisations must weigh up the cost of acquisition, implementation and maintenance of the control(s) against the 'value' of the information being protected;
2. Risk Transfer - This decision requires the risk to be transferred to another party that can effectively manage costs associated with the particular risk;
3. Risk Avoidance - Stop the activity that would give rise to the risk, thus eliminating the risk. Risk avoidance is not commonly selected as it typically results in not being able to exploit the associated opportunity; and

4. Risk Acceptance - This decision relies on the findings of the risk assessment and is applied when the level of risk is assessed within the business's defined risk tolerance level. However, the business may accept when it is not practical to avoid, treat or transfer the risk.

2.2.5 Selection and implementation of security measures

The appropriate security measures must be selected and implemented once security requirements have been identified. Security measures need to ensure risks are reduced to an acceptable level. The extent of the security measures required must be balanced against the potential business impact that may arise from security failures. Security measures can include local policies, standards, procedures, guidelines, practices, technological solutions and organisational structures. Measures will vary for different information systems and assets, depending on the criticality and sensitivity of the particular information asset.

2.2.6 Risk monitoring and review

Risks, threats and impacts will change over time and identified risks are to be reassessed to ensure the security measures selected remain appropriate and effective. Risks must be reviewed annually, or more frequently when major changes are made to information systems and assets.

2.3 Allocation of resources and training

Adequate resources (people, time, money) must be assigned to the operation of the ISMS/CSMS, including all security controls.

Information security training is required for all persons with access to NSW Health information to ensure procedures are followed to adequately protect information

2.4 Performance evaluation

NSW Health organisations must regularly collect and evaluate metrics on existing security measures: The evaluation of these metrics will lead to:

1. Improved information security processes – Quantify improvements in securing information and demonstrate quantifiable progress in information security objectives;
2. Increased accountability – By identifying specific security measures that are implemented incorrectly, not implemented or ineffective;
3. Greater support for decision making - Provide quantifiable information to the risk management process. Measure success/failure of investments and support resource allocation for future investments; and
4. Evidence of meeting requirements - Fulfilling ISMS/CSMS requirements and other applicable laws, rules and regulations.

2.5 Continual improvement

NSW Health Organisations must continually improve their ISMS/CSMS, including information security processes, techniques and controls. Continual improvement will be achieved through the ongoing processes of:

1. Risk assessment and treatment;
2. Evaluation of effectiveness of implemented security measures;
3. Corrective actions from internal audits and management reviews;
4. Reviewing and updating of information security documentation;
5. Training and awareness;
6. Review of information security incidents; and
7. Compliance reviews.

3 INFORMATION SECURITY INCIDENT RESPONSE PLAN

NSW Health Organisations must have an information security incident response plan that outlines the process for reporting and managing information security incidents, events and concerns from internal and external sources. Monitoring tools and processes must be in place for incident identification and response.

All users are responsible for reporting any information security concerns, events or incidents. Security events and incidents must be reported to eHealth NSW, Information Security Services within 48 hours and, to facilitate any investigation, as much relevant information as possible must be provided.

All reported information security concerns, events and incidents must be recorded in an appropriate register, which will be the official record and form the basis for evaluation and investigation. The register will be used to maintain the current status and the history of each incident as well as all decisions, recommendations and actions related to it.

The incident response plan must include the following steps:

1. Preparation;
2. Detection and Analysis;
3. Containment, Eradication, and Recovery; and
4. Post Incident Review.

3.1 Preparation

NSW Health Organisations must establish an information security incident response capability, separate to the security incident plan, so that they are ready to respond to incidents.

3.2 Detection and analysis

NSW Health Organisations must define the process for detecting and confirming an incident has occurred; categorising the nature of the incident and then prioritising the incident.

3.3 Containment, eradication, and recovery

NSW Health Organisations must identify the immediate response actions to deal with the information security incident. The primary objective is to confine any adverse impact to information systems and assets, followed by processes for the eradication of the threat and the return to the normal productive state of information systems and assets.

3.4 Post-Incident Review

NSW Health Organisations must compile a summary of actions and findings once the information security incident has been resolved. Any recommendations for changes to existing procedures or technology that will enhance the incident response plan must be documented.

4 ROLES AND RESPONSIBILITIES

Clearly defined roles and responsibilities ensure the proper protection of the information systems and assets of NSW Health.

4.1 Secretary, NSW Health

The Secretary, NSW Health must ensure all NSW Health Chief Executives establish, maintain and adequately resource an ISMS/CSMS. It is also the responsibility of the Secretary, NSW Health to ensure that the Chief Information Officer (CIO), NSW Health works with NSW Health Organisation Chief Executives and CIOs to implement this policy and that all NSW Health Organisations implement risk-based protections for information systems and assets.

The Secretary, NSW Health must ensure that all NSW Health Organisations comply with the NSW Cyber Security Policy. Reporting on compliance includes completing a yearly attestation report to be provided to Cyber Security NSW, which is completed by eHealth NSW on behalf of the Health Cluster. It is required that a copy of this report is included in the NSW Health annual report.

4.2 Chief Executives

Chief Executives must ensure that an ISMS/CSMS is established, adequate resources are allocated to implement the policy and associated framework, and there is appropriate resourcing and support of cyber security initiatives, including training and awareness and continual improvement initiatives.

It is also the responsibility of the Chief Executive, in collaboration with eHealth NSW, to ensure that their organisation complies with the *NSW Cyber Security Policy* and reports to the Secretary, NSW Health on compliance annually.

4.3 Chief Information Officer, NSW Health

The Chief Information Officer (CIO), NSW Health works with NSW Health Organisation Chief Executives and CIOs to implement this policy and ensures that all NSW Health Organisations implement risk-based protections for information systems and assets. This includes consideration of threats, risks and vulnerabilities that impact the protection of information systems and assets within their risk tolerance.

The CIO, NSW Health advises and guides NSW Health Organisation Chief Executives and CIOs on their responsibilities, which includes ensuring that all staff, including consultants, contractors, third parties and outsourced service providers, understand the cyber security requirements of their roles.

The CIO, NSW Health must also ensure a secure-by-design approach is in place for new initiatives and upgrades to existing systems and that all staff and providers understand their role in building and maintaining secure systems.

4.4 Director Information Security Services, eHealth NSW

The Director Information Security Services (ISS), eHealth NSW assists with defining and implementing risk-based protections for information systems and assets for NSW Health Organisations. Assistance and guidance is provided to NSW Health Organisations to implement policies, procedures, practices and tools that ensure compliance with this policy.

Responsibilities of the Director ISS, eHealth NSW include building an information security incident response plan that links NSW Health incident management and the whole of government cyber response plan. This allows the Director ISS, eHealth NSW to investigate, respond to and report on cyber security events within NSW Health and reports these incidents to the appropriate NSW Health governance forum and Cyber Security NSW.

The Director ISS, eHealth NSW must establish training and awareness programs to increase employees' cyber security capability and collaborate with NSW Health privacy, audit, information management and risk officers to protect NSW Health Organisation information systems and assets.

Other duties of the Director ISS, eHealth NSW include representing NSW Health Organisations on whole of government collaboration, advisory or steering groups, established by Cyber Security NSW as the central cluster Chief Information Security Officer (CISO) for NSW Health.

4.5 Data governance

The *NSW Health Data Governance Framework* outlines the roles and responsibilities involved in data governance and the structures in place to ensure effective and consistent management of the data assets of NSW Health.

The Framework facilitates data quality and comprehensiveness, appropriate access to data, information security, and standardisation of concepts.

Each data asset must have in place processes to protect the privacy and confidentiality of data through access management and security controls. This includes ensuring that the data is appropriately secured, backed up and disposed of according to agreed and documented protocols. Data must only be disclosed for the purpose for which it is collected. Alignment of data and IT governance must enforce regulatory, architectural and security compliance requirements.

The Framework also provides the 'Principles of Data Governance for NSW Health' that support the structured and consistent management of data assets and outlines the essential components of data governance, including description of the roles of Data Sponsor, Data Custodian and Data Steward.

The Data Sponsor is responsible for the control of strategic direction and undertaking duties of ownership that includes:

1. Enabling strategic management, governance and operation of the asset;
2. Providing direction and guidance, and authorising appropriate resources for management of the data asset; and
3. Appointing a Data Custodian and ensuring the Data Custodian's duties are fulfilled.

The Data Custodian is responsible for the day to day management and oversight of the asset, approval of access to data and the overall quality and security of the asset. This includes:

1. Ensuring any use of the data aligns with the purpose for which it is collected;
2. Establishing a data quality framework that ensures the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of the data;
3. Controlling access to data in compliance with all relevant legislation, policies, standards and any conditions specified by the Data Sponsor;
4. Regularly reviewing users with access to data and the ongoing need and appropriateness of access; and
5. Appointing a Data Steward.

The Data Steward is responsible for the day to day management and operation of the data asset, its completeness and quality. This includes:

1. Managing the data asset in compliance with all relevant legislation, policies, standards and any conditions specified by the Data Sponsor;
2. Co-ordinating stakeholder engagement and input into the business requirements for the data asset; and
3. Providing advice to the Data Custodian and Data Sponsor on the management of the data asset.

4.6 System administrators

System administrators need to be aware of, understand and follow acceptable procedures for granting/revoking access, identifying and resolving known vulnerabilities, and monitoring system access. They are responsible for developing practices and

procedures to support the policy and ensure compliance with the security requirements of information owners.

4.7 IT technical and support staff

IT support staff must manage confidentiality, integrity and availability of information systems. Staff are responsible for ensuring the appropriate access, delivery and ongoing support for systems, including applications, servers, networks, firewalls, routers and cloud services.

IT technical staff and system developers are responsible for delivering reliable software. Technical staff should understand the business use and risks associated with the technologies being used so that security solutions match the criticality and sensitive nature of the systems. They are responsible for developing practices and procedures to support the policy and ensure compliance with the security requirements of information owners.

4.8 Records and Information Managers

Records and Information Managers are responsible for maintaining a record and information management program in conformity with the standards and codes of best practice approved by NSW State Archives and Records. All disposal and destruction of records and information must be carried out in accordance with the relevant approved retention and disposal authority. They are responsible for developing practices and procedures to support organisation's records management policy and to ensure that records held in electronic (digital) or other technology dependent formats are accessible and protected for as long as they are required.

4.9 Users

Users of NSW Health information systems and assets play an important role in overall information security planning and risk management processes. Users must be aware of their responsibilities in relation to information security and privacy. Users have a role in identifying and reporting security concerns and incidents to management for investigation and review. Compliance with this policy and all relevant acts and regulations as they relate to information security is mandatory for all users.

4.10 Third party businesses and organisations, consumers and other agencies

The growing existence of inter-connected networks requires the extension of the 'boundaries' of NSW Health Organisations. All third parties must adhere to NSW Health and agency policies and procedures to ensure that adequate security controls are in place in the third-party environment.

4.11 Auditor

The role of independent reviewers and auditors is to assess the effectiveness and efficiency of implemented controls and whether controls are being adhered to. Independent reviewers and auditors must check compliance against policy and legislative

requirements. Review and audit reports should be noted by executive management and, if appropriate, remedial action taken.

The internal auditor will regularly review NSW Health Organisations' adherence to this policy and cybersecurity controls, from a risk management perspective.

5 RELATED DOCUMENTS

5.1 NSW Health policy directives and guidelines

Reference	Policy Document Title
PD2009_076	Communications - Use & Management of Misuse of NSW Health Communications Systems
PD2015_037	Data Collections – Disclosure of Unit Record Data for Research or Management of Health Services
PD2015_036	Privacy Management Plan
PD2015_049	NSW Health Code of Conduct
GL2019_002	NSW Health Data Governance Framework
PD2015_043	Risk Management - Enterprise-Wide Risk Management Policy and Framework – NSW Health
Privacy Manual for Health Information	

5.2 Relevant legislation – NSW

- *Crimes Act 1900*
- *Defamation Act 2005*
- *Government Information (Public Access) Act 2009*
- *Government Sector Employment Act 2013*
- *Health Records and Information Privacy Act 2002*
- *Privacy and Personal Information Protection Act 1998*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

5.3 Relevant legislation - Commonwealth

- *Cybercrime Act 2001*
- *Copyright Act 1968*
- *Privacy Act 1988*
- *Spam Act 2003*

5.4 NSW Government policies and directives

- Intellectual Property Management Framework for the NSW Public Sector
- Internal Audit and Risk Management Policy for the NSW Public Sector
- NSW Government Cyber Security Policy
- NSW Government: Information Classification, Labelling and Handling Guidelines

5.5 Standards

AS ISO/IEC 27001:2015. Information technology - Security techniques - Information security management systems – Requirements (this document is the same as ISO/IEC 27001:2013)

AS ISO/IEC 27002:2015. Information technology - Security techniques - Code of practice for information security management (this document is the same as ISO/IEC 27002:2013)

ISA/IEC 62443 - Series of standards, technical reports, and related information that define procedures for implementing secure Industrial Automation and Control Systems (IACS).