Metro North Information Security Strategy

Metro North Information Security Strategy (including Cyber Security)

V1.0 Effective: April 2023 Review: April 2024

Metro North Health | Queensland Government

Published by the State of Queensland (Metro North Hospital and Health Service), April 2023

For more information, contact:

Digital Metro North, Metro North Hospital and Health Service, Campbell Place, 153 Campbell St, Bowen Hills QLD 4006, email digitalmetronorth@health.qld.gov.au

An electronic version of this document is available at Health Service Strategy and Planning| Metro North Hospital and Health Service

Disclaimer:

The content presented in this publication is distributed by the Queensland Government as an information source only. The State of Queensland makes no statements, representations or warranties about the accuracy, completeness or reliability of any information contained in this publication. The State of Queensland disclaims all responsibility and all liability (including without limitation for liability in negligence) for all expenses, losses, damages and costs you might incur as a result of the information being inaccurate or incomplete in any way, and for any reason reliance was placed on such information.

Contents

Document details

Commercial-in-confidence

This document may contain commercial-in-confidence information. The document has been produced for the sole use of Metro North Hospital and Health Service and should not be provided to external organisations without the written approval of the Chief Digital Health Officer, MNHHS.

Version control

Version	Date	Prepared by	Comments
0.02	September 2019	Kamran Mustafa	Initial Draft
0.03	September 2019	Lisa Pomery	Additions of MNHHS focused and specific detail, focus on CIA and NIST
0.04	July 2022	Lisa Pomery	Update document
0.07	November 2022	Lisa Pomery	Following GSI team, and MNIMG feedback

Reviews

The following people have reviewed this document.

Name	Title / Role	Version	Date
MNIMG	ISMS Governance group - Endorsed	V1.0	December 2022
DCPCG	Digital Governance group - Endorsed	V1.0	March 2023

Approvals

The following officer has **approved** this document:

CDHO

Signature:	Signed version held on file	Business Area:	DMN
Name:	Jason Brown	Date:	_13/04/2023_________________
Position:	Chief Digital Health Officer	Contact Number:	(07)

The following officers have **endorsed** this document:

Chair MNIMG

Signature:	Signed version held on file	Business Area:	DMN
Name:	James Muller	Date:	12/04/2023
Position:	Clinical Informatics Director	Contact Number:	0409 059 135

ISMS lead

Signature:	Signed version held on file	Business Area:	DMN
Name:	Lisa Pomery	Date:	__9/12/2022____________
Position:	Delivery Stream Lead - ISMS	Contact Number:	(07) 3542 6322

Manager Cyber Security

Signature:	Signed version held on file	Business Area:	DMN
Name:	Chris Sheed	Date:	______14/04/2023___________
Position:	Manager Cyber Security	Contact Number:	0415 604 866

1. Introduction

1.1. Document purpose

This document sets out the Metro North Hospital and Health Service (MNHHS) Information Security Strategy. This strategy builds on the requirements under the Queensland Government (QG) IS18 policy and aligns with the MNHHS Strategy, objectives as well as those defined in the Queensland Health (QH) strategy, policies and standards. This is the start of moving from a reactive approach to a strategic planning approach based on risk.

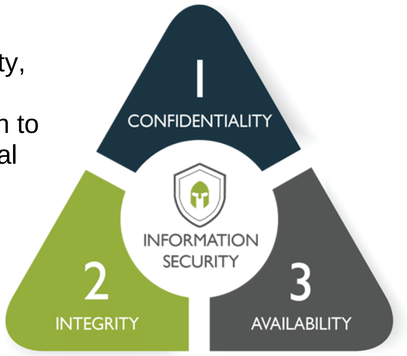
1.2. Intended audience

The audience for this document includes:

Audience	Explanation
All Metro North Staff	All staff need to be aware of information security in their day-to-day activities. This document will introduce elements both technical and cultural that will assist improving the human risk factors that are attributable to many information security events.

1.3. What is Information Security?

Information security is broadly defined as the measures used to protect the confidentiality, integrity and availability of information, systems and data from compromise (CIA triad). Information security and Cyber security are used interchangeably, however it is common to see information security encompassing both cyber security as well as security of physical and paper information. This can be further distilled into pre-emptive measures, such as the identification and treatment of risks to information, and reactive endeavours such as incident response and forensics capabilities. For MNHHS, it is about managing our partners and achieving the balance between delivering high quality healthcare and protecting our information assets.



CIA triad

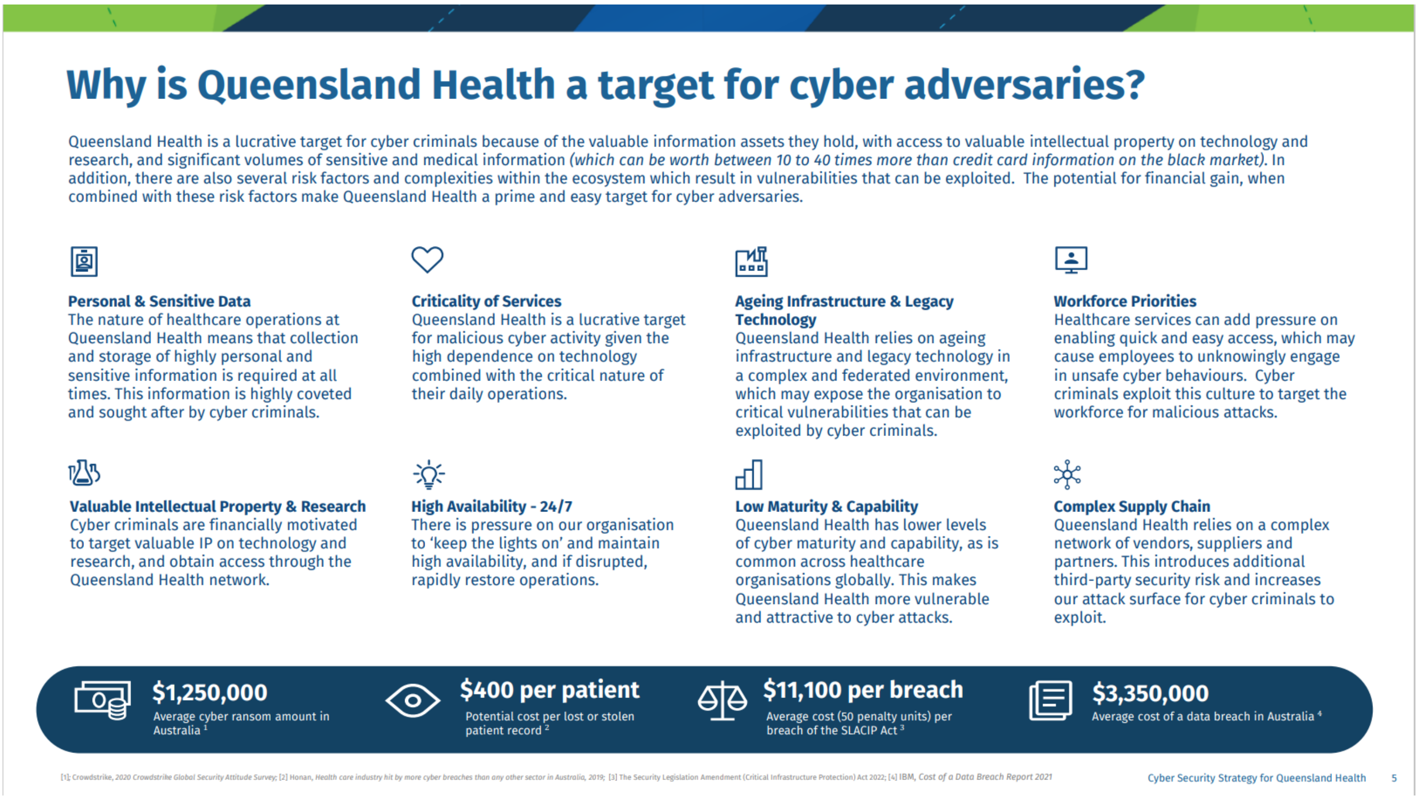
1.4. Why is Information Security important?

Ensuring our information is safe in each of the CIA domains is critical for the functioning of health care. Within MNHHS a breach of the CIA could mean reputational damage, non-compliance, legal and financial penalties and even be a contributing factor to patient harm. Ensuring the likelihood and consequences of information security risks are mitigated to an appropriate level is a critical function.

The role of information security within the healthcare industry is receiving greater priority than at any other time and this trend is likely to continue. Recent high-profile incidents, such as the 2022 Optus and Medibank information security breaches for which millions of Australians have been impacted, as well as the WannaCry ransomware attack of May 2017 which crippled the United Kingdom's National Health Service and the May 2018 recall of 500,000 Abbott pacemakers due to cyber security vulnerabilities, have brought this conversation into the mainstream. With each new day a multitude of disparate medical devices are being connected, both to the hospital networks under our control, and to private and public networks beyond our control. Many of these devices are low-cost/mass produced and have been designed and built devoid of robust security principles, such as the ability to patch and remediate identified vulnerabilities, or with uniform, default credentials. In devices such as heart and glucose monitors, pacemakers, and infusion pumps the consequences for patients can be dire. In turn, the inevitable loss of trust, reputational damage and potential financial impacts through litigation or legislative breaches can degrade outcomes for the healthcare sector in general.

Incidents like these have introduced the public to the reality that we are in an age where the risk of loss of life resulting directly from information and cyber security incidents is no longer science fiction and a direct safety risk.

With advances in clinical methodologies and supporting technology, the reliance on these systems becomes more critical for the effective delivery of advanced healthcare. MNHHS faces an ever-increasing need to be resilient in an aggressive and constantly changing threat environment to protect systems and data that are continually growing in volume, distribution, and in value to cybercriminals.



Why is Queensland Health a target for cyber adversaries?

Queensland Health is a lucrative target for cyber criminals because of the valuable information assets they hold, with access to valuable intellectual property on technology and research, and significant volumes of sensitive and medical information *(which can be worth between 10 to 40 times more than credit card information on the black market).* In addition, there are also several risk factors and complexities within the ecosystem which result in vulnerabilities that can be exploited. The potential for financial gain, when combined with these risk factors make Queensland Health a prime and easy target for cyber adversaries.

Personal & Sensitive Data
The nature of healthcare operations at Queensland Health means that collection and storage of highly personal and sensitive information is required at all times. This information is highly coveted and sought after by cyber criminals.

Criticality of Services
Queensland Health is a lucrative target for malicious cyber activity given the high dependence on technology combined with the critical nature of their daily operations.

Ageing Infrastructure & Legacy Technology
Queensland Health relies on ageing infrastructure and legacy technology in a complex and federated environment, which may expose the organisation to critical vulnerabilities that can be exploited by cyber criminals.

Workforce Priorities
Healthcare services can add pressure on enabling quick and easy access, which may cause employees to unknowingly engage in unsafe cyber behaviours. Cyber criminals exploit this culture to target the workforce for malicious attacks.

Valuable Intellectual Property & Research
Cyber criminals are financially motivated to target valuable IP on technology and research, and obtain access through the Queensland Health network.

High Availability - 24/7
There is pressure on our organisation to ‘keep the lights on’ and maintain high availability, and if disrupted, rapidly restore operations.

Low Maturity & Capability
Queensland Health has lower levels of cyber maturity and capability, as is common across healthcare organisations globally. This makes Queensland Health more vulnerable and attractive to cyber attacks.

Complex Supply Chain
Queensland Health relies on a complex network of vendors, suppliers and partners. This introduces additional third-party security risk and increases our attack surface for cyber criminals to exploit.

$1,250,000
Average cyber ransom amount in Australia [1]

$400 per patient
Potential cost per lost or stolen patient record [2]

$11,100 per breach
Average cost (50 penalty units) per breach of the SLACIP Act [3]

$3,350,000
Average cost of a data breach in Australia [4]

[1]; Crowdstrike, *2020 Crowdstrike Global Security Attitude Survey;* [2] Honan, *Health care industry hit by more cyber breaches than any other sector in Australia, 2019;* [3] The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022; [4] IBM, *Cost of a Data Breach Report 2021*

Cyber Security Strategy for Queensland Health 5

From QH Cyber Security Strategy 2022 - 2031

1.5. MNHHS relevant strategic objectives to Information security

Our MNHHS strategic plan identifies strategic risks and objectives.
OBJECTIVE 2 aims to improve health equity, access, quality, safety and health outcomes.

Those relevant to this body of work are:

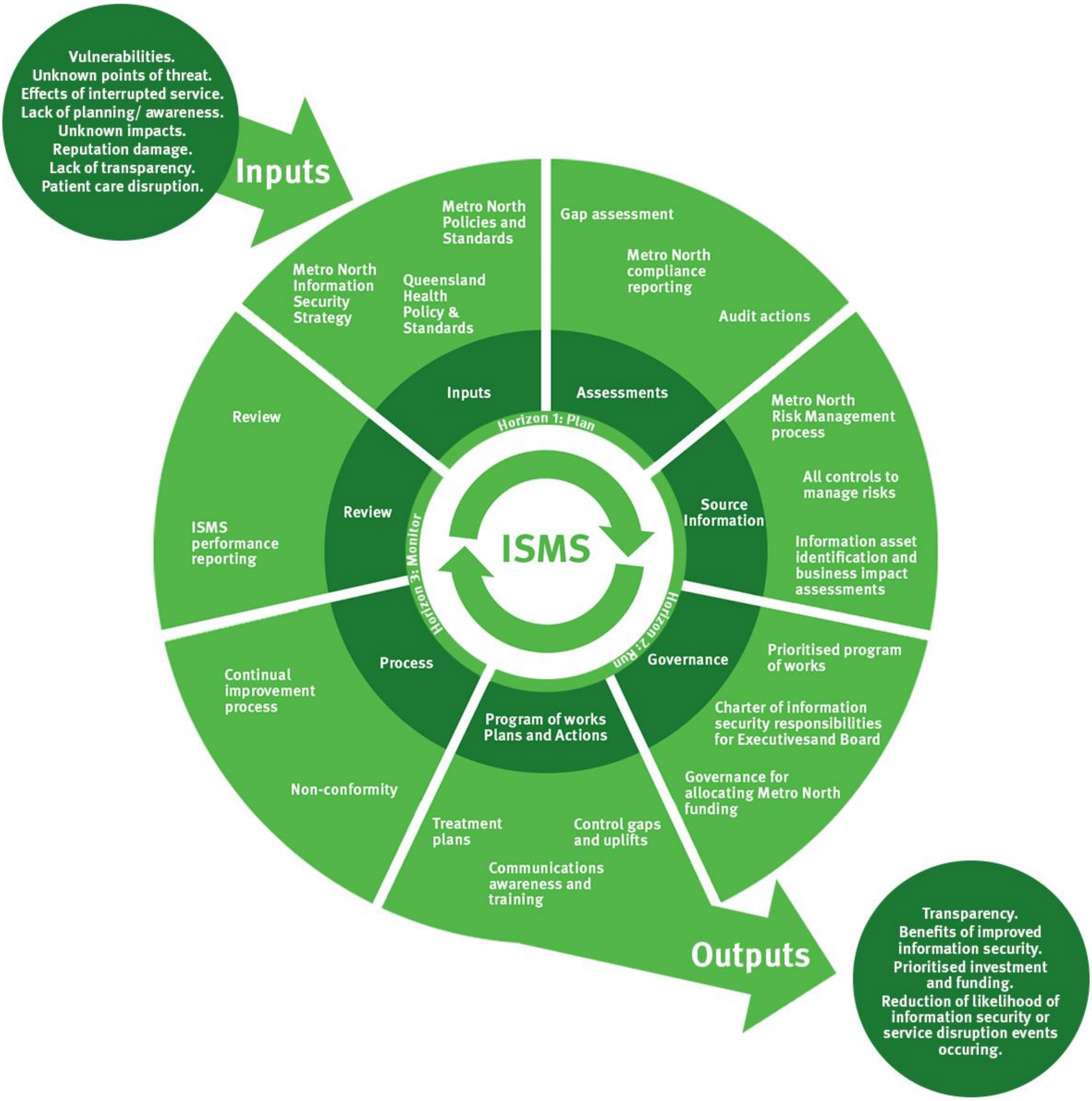
- Digital Transformation and Cyber Security: Failure to successfully execute digital transformation would adversely impact patient outcomes, service delivery, research and clinical partnerships and organisational viability. Inadequate processes to prevent and/or respond to cyber threats may result in loss or corruption of sensitive information and cause critical service disruption compromising patient care and organisational performance.
- Asset and Infrastructure: Ageing infrastructure with inadequate funding may lead to Metro North carrying an increasing liability for building asset performance resulting in impacts on clinical service delivery. (Aging unsupported infrastructure is likely to have unpatched vulnerabilities increasing the likelihood of cyber security incidents)
- Adaptability: Failure to embed an organisational culture that is responsive and adaptable to change will impact on the organisation’s ability to respond to external forces, including a pandemic, and capitalise on opportunities when presented.

1.6. MNHHS Information security vision

To support our Health service, staff, patients and community by providing an appropriate amount of information security as determined by the assessment of the environment using an agile, risk-based approach.

1.7. MNHHS Information security approach

Using the strength of the QH federated network and understanding the rapid and evolving nature of the information security environment, MNHHS will build strong foundations to establish the risk based, agile approach to information security. The diagram shows the planned approach to run the MNHHS ISMS ongoing function. ISMS is not a project that can be implemented and completed, it is a new service function focusing on information security for MNHHS.


Vulnerabilities.
Unknown points of threat.
Effects of interrupted service.
Lack of planning/ awareness.
Unknown impacts.
Reputation damage.
Lack of transparency.
Patient care disruption.
Inputs
Metro North Policies and Standards
Metro North Information Security Strategy
Queensland Health Policy & Standards
Gap assessment
Metro North compliance reporting
Audit actions
Inputs
Assessments
Horizon 1: Plan
Metro North Risk Management process
All controls to manage risks
Information asset identification and business impact assessments
Source Information
Review
Review
ISMS performance reporting
Horizon 3: Monitor
ISMS
Horizon 2: Run
Governance
Prioritised program of works
Charter of information security responsibilities for Executivesand Board
Governance for allocating Metro North funding
Process
Continual improvement process
Non-conformity
Program of works Plans and Actions
Treatment plans
Control gaps and uplifts
Communications awareness and training
Outputs
Transparency.
Benefits of improved information security.
Prioritised investment and funding.
Reduction of likelihood of information security or service disruption events occuring.

MNHHS ISMS Approach

Noting as controls are usually at MNHHS level and often spread diversly across variety of levels and areas, a MN quarantined pool of funding to be allocated on a risk-based approach for MNHHS benefit is requested to ensure, that funding is available to mitigate MNHHS wide risks, when local funding is not available in all areas.

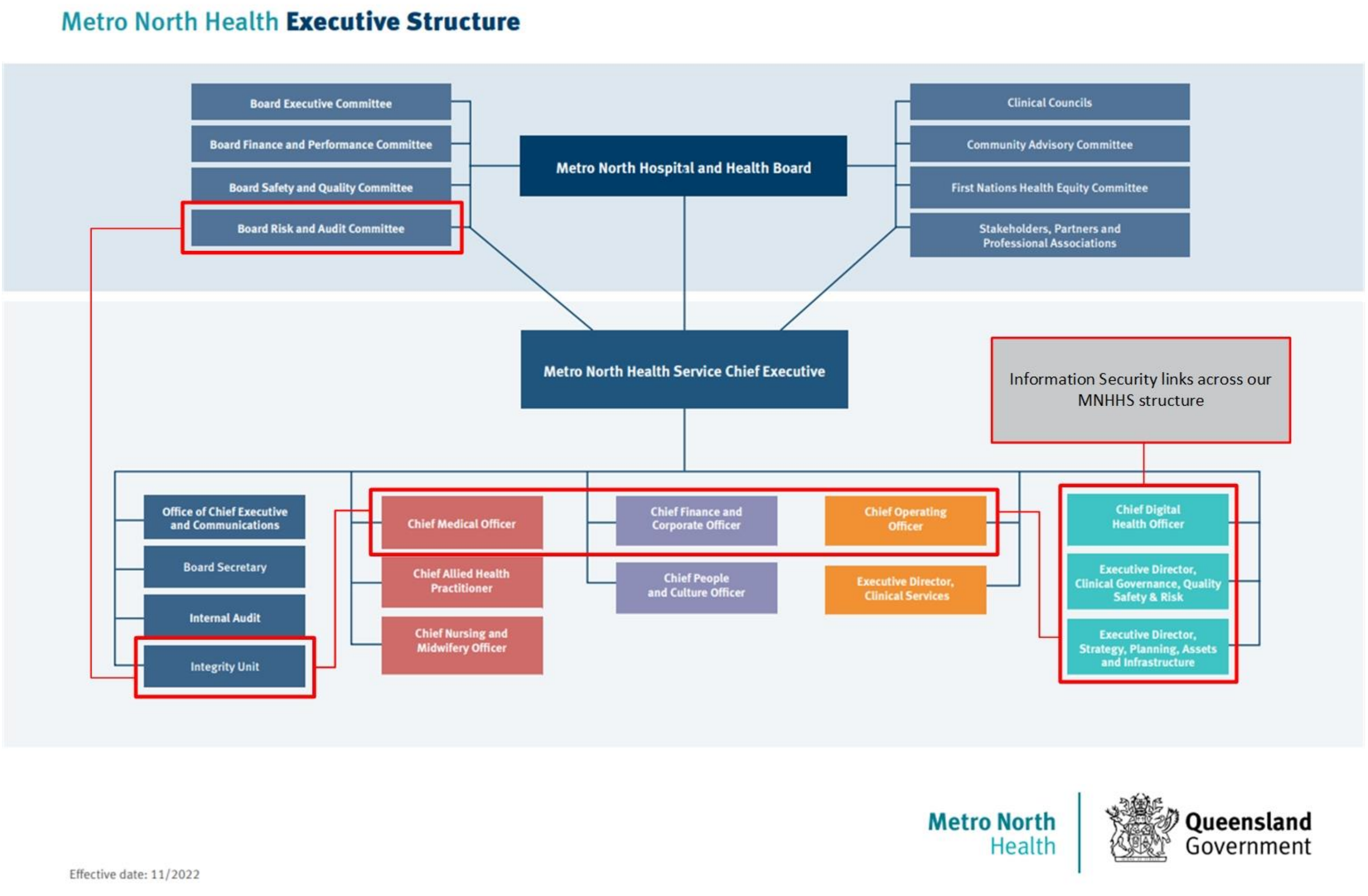
2 Information Security Landscape

2.1 Metro North Hospital and Health Service

MNHHS delivers responsive, integrated, and connected care to local communities and provides specialty services for patients throughout Queensland, Northern New South Wales and the Northern Territory. MNHHS services a local population over 900,000, from north of the Brisbane River to north of Kilcoy. The population of MNHHS is expected to reach over 1.1 million people by 2026.

MNHHS services incorporate all major health specialties including medicine, surgery, psychiatry, oncology, women’s and children, trauma, subacute and more than 30 sub-specialties. MNHHS facilities and services include The Royal Brisbane and Women’s (RBWH) and The Prince Charles Hospital (TPCH), both quaternary/tertiary referral facilities that provide advanced levels of highly specialised health care. Redcliffe and Caboolture Hospitals are regional hospitals, and Kilcoy Hospital is a community hospital. Mental health, oral health, community, Indigenous and subacute services are provided from many sites including hospitals, 11 community health centres, residential and extended care facilities and mobile service teams.

MN32 strategic plan and the Digital Metro North Strategic plan highlight that MNHHS is moving towards a digital hospital environment. This means that more and more of our information and the information we hold as custodians for our patients and staff is transitioned to electronic means. Although information security is always important, with traditional security of location and confidentiality of patient paper records still being of critical importance, the element of moving to the digital, more electronic records brings additional chances of information security threats and opportunities which will require management.


Metro North Health Executive Structure
Board Executive Committee
Board Finance and Performance Committee
Board Safety and Quality Committee
Board Risk and Audit Committee
Metro North Hospital and Health Board
Clinical Councils
Community Advisory Committee
First Nations Health Equity Committee
Stakeholders, Partners and Professional Associations
Metro North Health Service Chief Executive
Information Security links across our MNHHS structure
Office of Chief Executive and Communications
Board Secretary
Internal Audit
Integrity Unit
Chief Medical Officer
Chief Allied Health Practitioner
Chief Nursing and Midwifery Officer
Chief Finance and Corporate Officer
Chief People and Culture Officer
Chief Operating Officer
Executive Director, Clinical Services
Chief Digital Health Officer
Executive Director, Clinical Governance, Quality Safety & Risk
Executive Director, Strategy, Planning, Assets and Infrastructure
Metro North Health
Queensland Government
Effective date: 11/2022

2.2 Digital Metro North

Digital Metro North – Technology Services plans, co-ordinates, delivers and supports ICT services to enable MNHHS to deliver health care and services. Critical to the success of Technology Services is working closely with clinical and support staff across MNHHS facilities and service lines to ensure ICT services remain responsive, relevant, and aligned with business priorities.

Information Security services are co-ordinated and managed through MNHHS using partners, planning and operational activities at both MNHHS, eHQ and QH levels. ISMS is the Information Security Management System which is the mandated framework QH use to taking a risk-based approach to information security. ISMS looks at the security of all information including digital and paper and as such a coordinated approach is needed both within MNHHS as well as with vendors, and partners such as eHQ and BTS.

Importantly the MNHHS data custodianship policy identifies data custodians which are divided into the broad domains of:

1. Corporate Administration - Chief Finance and Corporate Officer, Metro North
2. Patient Care - Executive Director Medical Services, Metro North; or Delegates – Directorate, Directors Clinical Health Information Services.
3. Research - Executive Director Research, Metro North

Policy: Data Custodianship 004570 | Metro North Hospital and Health Service

Data Custodian and Application Custodian 005836 (health.qld.gov.au)

The MNHHS ISMS manual identifies the management of the ISMS both at MNHHS and QH levels and the linkages between the organisations in a federated model.

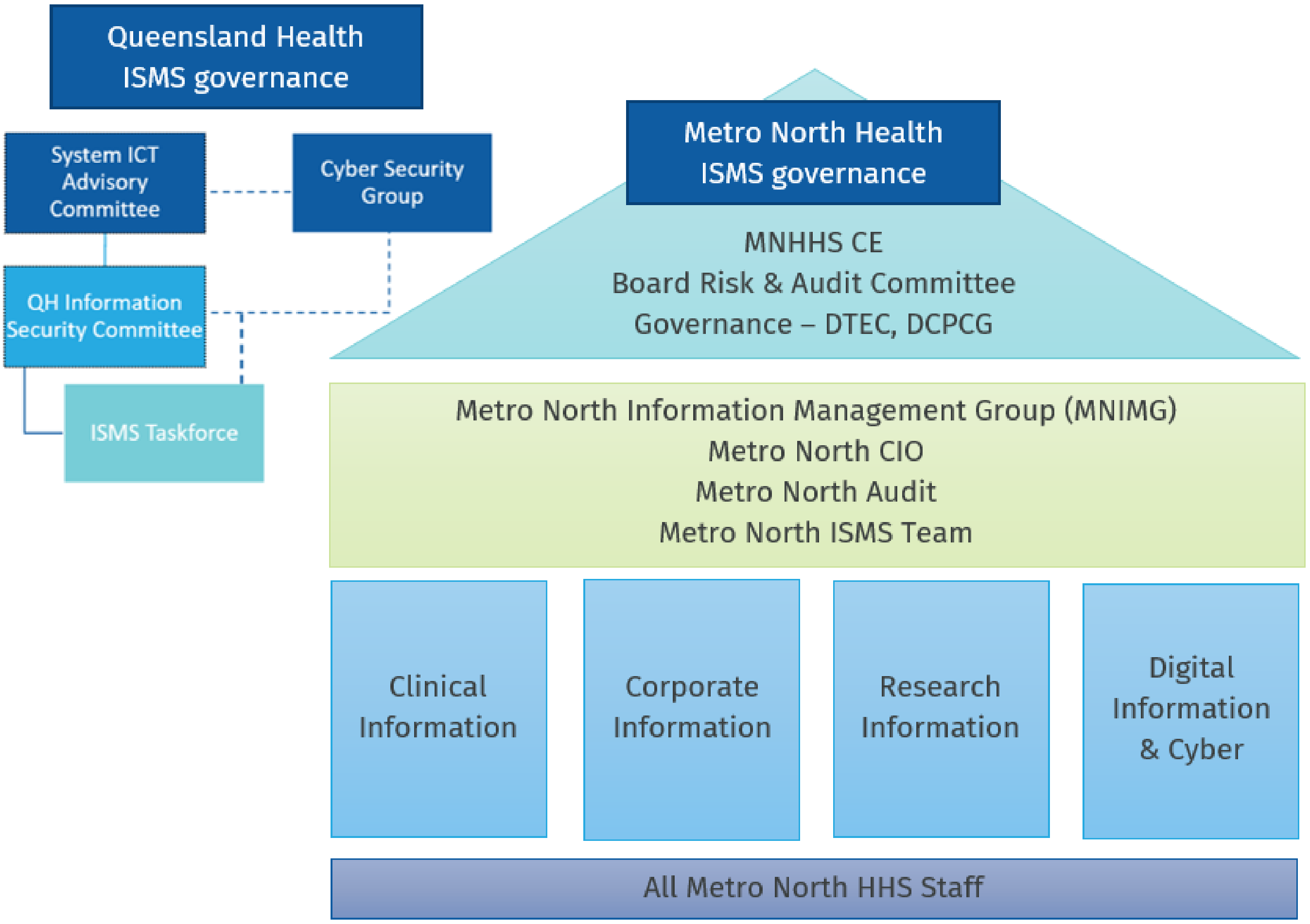

Queensland Health ISMS governance
System ICT Advisory Committee
Cyber Security Group
QH Information Security Committee
ISMS Taskforce
Metro North Health ISMS governance
MNHHS CE
Board Risk & Audit Committee
Governance – DTEC, DCPCG
Metro North Information Management Group (MNIMG)
Metro North CIO
Metro North Audit
Metro North ISMS Team
Clinical Information
Corporate Information
Research Information
Digital Information & Cyber
All Metro North HHS Staff

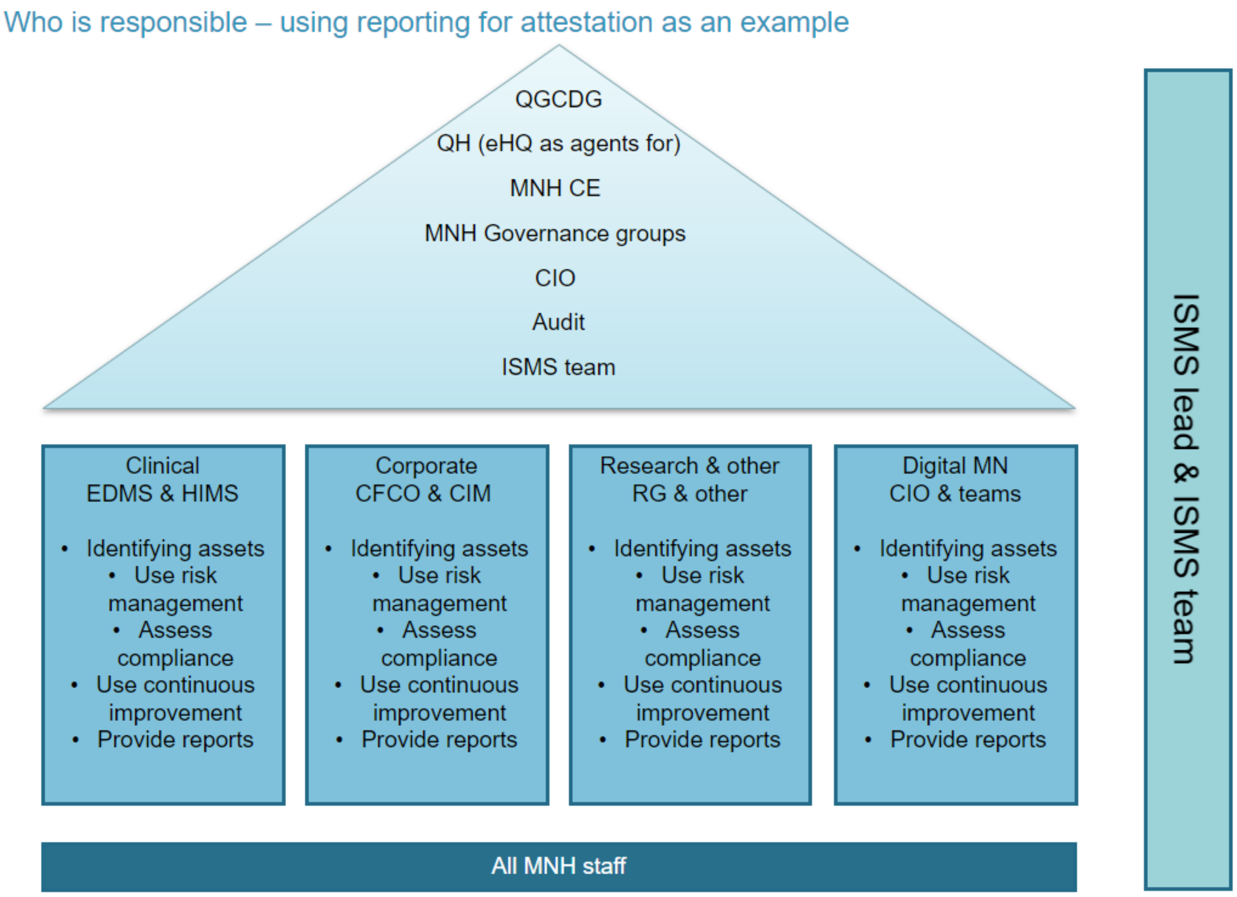
Figure 1 – Metro North ISMS Organisational structure

Extract from the MNHHS ISMS Manual

2.2.1 Current Information Security Service Partners and Suppliers

The information security landscape at MNHHS relies on our partners and third party suppliers to deliver and manage a range of services. QH hold the ISMS framework as part of the QGCIO push towards a whole of government risk-based approach to cyber. eHQ are leading the whole of QH ISMS function under a federated model where impacts are on an enterprise level including enterprise systems and services managed by eHQ and supplied to the HHSs.

Interested parties internal to MNHHS are:



Who is responsible – using reporting for attestation as an example

QGCDG

QH (eHQ as agents for)

MNH CE

MNH Governance groups

CIO

Audit

ISMS team

Clinical
EDMS & HIMS

- Identifying assets
- Use risk management
- Assess compliance
- Use continuous improvement
- Provide reports

Corporate
CFCO & CIM

- Identifying assets
- Use risk management
- Assess compliance
- Use continuous improvement
- Provide reports

Research & other
RG & other

- Identifying assets
- Use risk management
- Assess compliance
- Use continuous improvement
- Provide reports

Digital MN
CIO & teams

- Identifying assets
- Use risk management
- Assess compliance
- Use continuous improvement
- Provide reports

All MNH staff

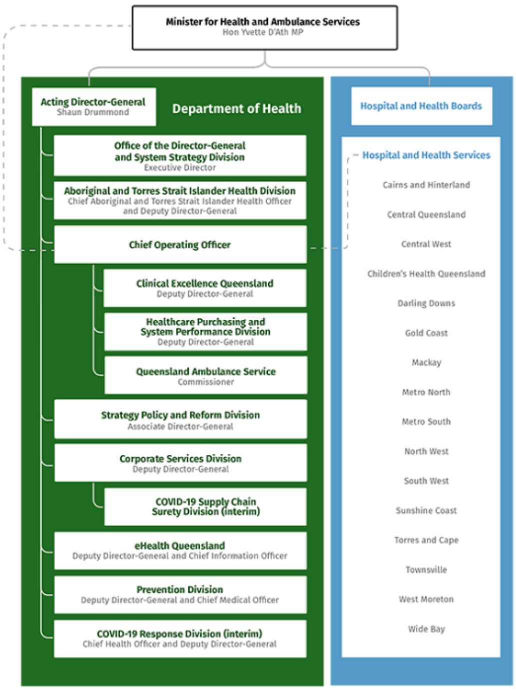
ISMS lead & ISMS team

Critical external parties include (but not limited to):

1. eHealth Queensland (eHQ):
   - Network security and Monitoring of QH network
   - Risk assessments for enterprise systems
   - End-user device patching for SoE devices
   - Anti-virus management for SoE devices
   - Email management
   - Internet and proxy services of QH network
   - Security incident management for QH network
   - Security awareness and training for QH
   - Penetration testing (procurement)
   - Identity management and other Essential 8 services
2. Biomed Technology Services (BTS):
   - Medical device assessment, installation and maintenance - (Health Technology (Medical Devices) Management 006174)

2.3 QH Cyber Security

The MNHHS ISMS is part of a federated government network. The setup is unique for QH and understanding the landscape in which it has been created is critical.


Minister for Health and Ambulance Services
Hon Yvette D'Ath MP
Acting Director-General
Shaun Drummond
Department of Health
Office of the Director-General and System Strategy Division
Executive Director
Aboriginal and Torres Strait Islander Health Division
Chief Aboriginal and Torres Strait Islander Health Officer and Deputy Director-General
Chief Operating Officer
Clinical Excellence Queensland
Deputy Director-General
Healthcare Purchasing and System Performance Division
Deputy Director-General
Queensland Ambulance Service
Commissioner
Strategy Policy and Reform Division
Associate Director-General
Corporate Services Division
Deputy Director-General
COVID-19 Supply Chain Surety Division (interim)
eHealth Queensland
Deputy Director-General and Chief Information Officer
Prevention Division
Deputy Director-General and Chief Medical Officer
COVID-19 Response Division (interim)
Chief Health Officer and Deputy Director-General
Hospital and Health Boards
Hospital and Health Services
Cairns and Hinterland
Central Queensland
Central West
Children's Health Queensland
Darling Downs
Gold Coast
Mackay
Metro North
Metro South
North West
South West
Sunshine Coast
Torres and Cape
Townsville
West Moreton
Wide Bay

Authorised by the Director-General, Queensland Health on 21 April 2022

Queensland Health (QH) is a term used to describe the health services funded by the Queensland government. This includes government agencies (Department of Health DoH) and statutory bodies (Hospital and Health Services HHS) who all report to the QH minister. (Queensland Health organisational structure | Queensland Health)

The HHSs were established in 2012 under the Hospitals and Health Board Act which divides the management of the local hospital services into 16 individually run organisations all of which report through individual Chief Executives and boards to the QH minister, as well as the DoH reporting through the Director General to the QH minister. (Hospital and Health Boards Act 2011 (legislation.qld.gov.au)) This also includes ownership and management of information at HHS level.

In this setup eHealth Queensland (as part of DoH) operate with 3 responsibilities:

1. As an enterprise provider of enterprise systems, the network, SoE workstations and servers etc. – Vendor essential 8 (excluded from the HHS essential 8 report) – some of this is described in the shared SOA, but currently it is not all defined.
2. As the agent to aggregate the details for the federated QH ISMS, HSD and coordinator of QH policies and standards and enterprise data custodians.
3. As the manager of ICT for DoH

In 2018, the Queensland Government (QG) embarked on a major revision of the Information Security Policy IS18:2018 (released in 2019). Information security policy (IS18:2018) | Queensland Government Enterprise Architecture (qgcio.qld.gov.au) This policy change was made by the Queensland Government Customer and Digital Group (QGCDG) which was established to ensure the governments' ICT investments are appropriate and reliable. QGCDG provides advice to QG agencies in adopting better practice for ICT investment, managing risks and setting ICT strategy, policy and standards. About us | Queensland Government Enterprise Architecture (qgcio.qld.gov.au)

In 2019, eHealth Queensland (as part of the Department of Health) published an updated QH Information Security Policy (QH-POL-468:2019) which mandated the use of an ISMS Information Security Management System in line with the QG IS18:2018. https://www.health.qld.gov.au/__data/assets/pdf_file/0041/859595/qh-pol-468.pdf The mandate was implemented across both Department of Health (DoH) and the Health and Hospital Services (HHS) through a new Health Service Directive (HSD) – Enterprise ICT Governance HSD which mandated a range of policies and standards to enable standardisation across all of the federated Queensland Health model.
Enterprise information, communications and technology (ICT) governance | Health service directive | Queensland Health

This HSD describes the requirements through policy and standards of Queensland Health which encompasses both DoH and HHS. ICT policies | Queensland Health Note that some of those listed have a scope of DoH – in which case they are NOT applicable for the HHS. However, if HHSs wish to use DoH standards or policies, they can use them rebranded, but must not reference them directly as DoH standards and policies. The standards and policies are only applicable if the scope includes the HHS – this is indicated in the selection box for HHS/DoH, noting that all the headers say QH.

QH level ICT governance with DoH as the agents :
Department of Health Report Publication template
System ICT Governance committees - eHealth Queensland

QH enterprise applications managed by DoH / eHQ (eHQ act as vendors for service provided to HHS):
Queensland Health Applications Index | Queensland Health Intranet

The 2022 federal Security of Critical Infrastructure (SOCI) act introduces this risk-based requirement for information security against our nations critical assets and ISMS will fulfil this requirement for the cyber security component. Other components of this risk-based approach – personnel, supply chain, physical and natural will be addressed outside of Information Security but using the same risk-based approach. Of note is BTS: Biomedical Technology Services, which like eHQ, is part of DoH and are a service provider to HHSs for managing medical devices. Currently, it is up to the HHS to request from BTS their compliance with the critical security control set known as the Essential 8 (E8) as in a vendor relationship.

eHQ and BTS provide some to most of the ICT services at each HHS. BTS devices currently are to be included within the HHS ISMS, but the services provided by eHQ are excluded from the HHS ISMS and are included only in the ISMS produced by eHQ (at a whole of state level). This means the HHS ISMS is a listing of the exceptions from the QH norm, that are not covered by the enterprise services provided by eHQ.

The new eHQ cyber security strategy focuses on the E8 controls eHQ are uplifting to manage the applications and devices eHQ provide to and managed for DoH and the HHSs. The MNHHS Information security strategy utilises these initiatives and fills the gaps between the eHQ offer and the requirements of the HHS using a risk-based approach.

3 Queensland Health Information Security Policy

3.1 Information Security Management System (ISMS)

Information Standard 18 (IS18:2018) is the information security policy for Queensland Government. This policy has been reviewed and refreshed to keep pace with the changing requirements of government. This has resulted in a greater focus on risk management and agency accountability. The changes to IS18 have seen strengthened alignment with the current Australian and international standard for information security management systems (ISO27001).

The Queensland Security Cabinet Committee endorsed a set of principles for cyber security in 2017.

Queensland Government Cyber Security Principles are:

- Cyber security is a CEO and leadership responsibility.
- Cyber security risk management and governance are to be embedded in agency management processes.
- Transparency of an agency's cyber risk and remediation is essential to ongoing improvement.
- Cyber security threat and incident information is proactively shared between Queensland Government agencies to help strengthen our government-wide defences.

3.2 Queensland Health Implementation

The whole of Queensland Health ISMS will implement one standardised ISMS with a suite of supporting standards, procedures and guidelines covering the whole agency. The eHQ Cyber Security Group will coordinate the approach across Queensland Health for the QH ISMS implementation, in addition to reporting to the Queensland Government Customer and Digital Group (QGCDG). MNHHS will localise the implementation of the minimum set of requirements set out in the standards based on the MNHHS risk appetite and tolerance and are responsible for the MNHHS ISMS function in alignment with the QH ISMS function.

As a result of the federated model of QH, MNHHS needs to provide a minimum level of compliance to the QH Information security policy.

The purpose of this policy is to ensure Queensland Health protects its information against unauthorised access, use (including loss of availability for appropriate use), disclosure, disruption, modification, perusal, inspection, recording, destruction, damage (malicious or accidental), fraud or a breach of privacy. This policy and its supporting standards enable a strong security culture, which will reduce risk and ensure all staff are meeting their responsibilities and duty of care as set out in the relevant Code of Conduct.

3.2.1 Queensland Health Information Security Principles:

- comply with applicable legislative and regulatory security requirements
- right information is accessed by the right people in the right place at the right time
- coordinate information security activities across Queensland Health
- manage information security risks effectively
- establish an effective information security culture regularly review and improve information security performance and capability
- provide health care practitioners an environment where the organisation can perform their work in a secure manner.

3.2.2 QH Information Security Objectives

- use a risk and privacy-based approach to protect confidentiality, integrity and availability of information assets and ICT assets
- implement a holistic risk management approach to information assets and ICT assets, through systematically assessing, monitoring, and treating information security risks, and improving controls, while protecting patients, employees and organisations from real impacts
- define roles and responsibilities within Queensland Health and any third-party service providers.

3.2.3 QH Information Security Requirements

- There is a Queensland Government requirement for Queensland Health to establish an Information Security Management System (ISMS) in line with the international standard ISO 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements*.
- The Queensland Health ISMS contains the minimum requirements that all HHSs and the Department of Health must comply with.
- Using the ISMS risk framework:
- each HHS must undertake a risk assessment to determine if the Queensland Health ISMS meets their business requirements and, where necessary, develop local policy artefacts to address any gaps identified
- all HHS and Department of Health staff must implement information security training commensurate with their risk appetite.
- Each HHS must provide, accurate and comprehensive information to eHealth Queensland to enable Queensland Health to meet the mandated reporting requirements defined in the Queensland Government Enterprise Architecture ICT Profiling Standard.
- Each HHS must report quarterly to the Cyber Security Group, eHealth Queensland, to ensure the Director General has state-wide oversight of information security risks, incidents and issues.
- All actual security incidents or security vulnerabilities must be reported to the Cyber Security Group, eHealth Queensland; Anything rated High or Very High is to be reported immediately or within the timeframes stated in the Technical Vulnerability Management Standard and Information Security Incident Management Standard.
- Queensland Health shall continually improve the suitability, adequacy and effectiveness of the ISMS.

4 MNHHS Information Security Action Plan

Using the fundamentals of cyber security NIST framework (identify, protect, detect, respond, recover), and acknowledging that cyber security is always a balance between investment and appropriate protection, requirements have been identified to meet the current MNHHS risk appetite for cyber security set by the MNHHS board.

- Low for critical assets and infrastructure and system continuity and
- Very Low for legislative compliance.

These are taken in alignment with the QH principals of using a risk-based approach as defined in the MNHHS ISMS which will drive the prioritisation of these initiatives using a risk-based approach.

These statements need to be balanced with MNHHS's significant appetite for risks and opportunities associated with being innovative in the pursuit of organisation goals and opportunities for improved clinical efficiencies and outcomes and MNHHS's significant appetite for pursuing opportunities surrounding digital innovations that enhance service delivery. Both of which further establish the critical need for strong digital and information security measures to support MNHHS's drive for innovation with strong foundations of information security fundamentals.

4.1 Foundational work

This Foundational work is the organisational development work that sits outside of the traditional NIST framework. These are elements that require establishment or continual improvement processes to ensure appropriate information security as this is an ever-changing field.

Current state:

- Governance is established as a federated model with QH, with QH providing policies and standards as a measure for compliance and reporting on both MNHHS and QH levels
- Information Security resourcing is extremely limited and has no dedicated funding for uplifting MNHHS wide information security controls.
- ISMS has been implemented with only a small subset of the information currently assessed with much more work to be undertaken, and currently no resource to maintain as BAU
- Fundamentals of risk management in place, with key areas requiring uplift
- Initial reporting requirements established with additional MNHHS areas to be onboarded and ensure appropriate accountability is achieved.

Initiatives / control uplifts / improvements:

4.1.1 Continue the establishment of the MNHHS ISMS in accordance with ISO 27001 (including shared QH policy and standards, shared Statement of Applicability, MNHHS control monitoring, reporting, gap assessments and continual improvements)

4.1.2 Uplift MNHHS risk management including understanding of using risk for prioritisation of control uplift and investments, including education.

4.1.3 Business case for delivering an ongoing team for ISMS and to deliver information security initiatives for MNHHS

4.1.4 Ensure reporting data is accurate and available to ensure compliance reporting can be achieved and accountable staff confirm the data in a timely fashion

Aligned risks:
Strategic : Information Security (Cyber Security) High (20)
Organisational : Clinical Information Management High (18)
Organisational : Corporate Information Management (Provisional)
Organisational : Cyber Security High (18)

KPIs:

1. MNHHS ISMS and compliance monthly reporting is agreed and achieved
2. Three new MNHHS areas are identified and onboarded with compliance reporting

4.2 Identify

The Identify Function assists in developing an organisational understanding to managing information security risk to systems, people, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related information security risks enables an organisation to focus and prioritise its efforts, consistent with its risk management strategy and business needs.

Outcome Categories within this Function include:

- Identifying physical and software assets to establish the basis of an Asset Management program including all users, information assets, dispensations and exemptions.
- Identifying options for network discovery, including devices (including BTS) with a process to identify ownership of devices and applications, both within the network and via SAAS
- Identifying information security policies established at QH level to define the Governance program within the federated environment as well as identifying legal and regulatory requirements regarding the information security capabilities of the organization (Gap analysis) including confirming processes for adding and removing users' devices and applications are appropriate for purpose
- Identifying asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for the organizations Risk Assessment

Current state:

- Only limited manual mechanisms of identification of people, software, devices, users, including network scanning.
- Complex environment with eHQ, vendors and local assets with a variety of support mechanisms
- Complexity in that not all ICT purchasing is centralised with many departments running their own ICT units and managing information locally, without the oversight of compliance and governance.
- Working with eHQ and QH to establish standards in order to set the baseline to measure our compliance against
- Very few options to be able to identify vulnerabilities and threats, with a large amount of work to do to identify the risks

Initiatives / control uplifts / improvements:

4.2.1 MNHHS risk assessments (initially all critical applications – prioritisation based on risk and resourcing)

4.2.2 MNHHS information asset identification (initially all critical applications)

4.2.3 Network discovery tool to identify all devices on the network (including BTS) and a process to identify ownership of the devices to ensure compliance.

4.2.4 Application discovery tool

4.2.5 Network traffic packets discovery tool to assist with identifying SAAS and staff education around the governance and compliance required

4.2.6 Work with BTS and other vendors (including eHQ), as well as throughout MNHHS teams to establish an appropriate process and reporting to ensure compliance

Aligned risks:
Organisational : Shadow IT Medium (12)
Organisational : Lack of visibility of eHealth Queensland ICT risks which have direct impacts on MNHHS Medium (11)
Operational : Asset lifecycle management (ALARP Low)
Operational : Medical device safeguards and system maintenance are not consistently completed Medium (12)

KPIs:

1. Assess options for automatic discovery tool for devices and software ensuring increase in number identified each month for investment and project initiation
2. Each month risks, treatments and controls are reviewed and added or ALARP'ed as appropriate (Minimum 1/mth)

3. Increase number of vendors (inc BTS) contributing to compliance reporting (Minimum 1/mth

4.3 Protect

The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential information security event.

Outcome Categories within this Function include:

- Protections for Identity Management and Access Control within the organization including physical and remote access
- Empowering staff within the organization through Awareness and Training including role based and privileged user training
- Establishing Data Security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
- Implementing Information Protection Processes and Procedures to maintain and manage the protections of information systems and assets
- Protecting organizational resources through Maintenance, including remote maintenance, activities
- Managing Protective Technology to ensure the security and resilience of systems and assets are consistent with QH and MNHHS organizational policies, procedures, and agreements

Current state:

- Reliance on eHQ work
- limited awareness of some policy and standards with not all of MNHHS ICT bodies of work processing through the governance and compliance processes

Initiatives / control uplifts / improvements:

4.3.1 Implement eHQ control uplifts, Privileged Access Management (PAM), Identity Access Management (IAM), firewall upgrades

4.3.2 Review current and new approval process for architecture and the process if the architecture is not secure

4.3.3 Continue with the Cyber governance education and awareness plan

4.3.4 Conduct gap assessments and control maturity assessments for MNHHS

4.3.5 Implement, asses, and extend upon eHQ provided software to enable automated protection to MNHHS devices.
Review which eHQ offer can be extended to MNHHS supported devices, and when not possible perform risk assessments to determine other possible treatments

4.3.6 Ensure vendor compliance, audit and reporting are appropriate

Aligned risks:
Organisational : Separation process - identification and removal of IT access Medium (12)
Operational : Lack of compliance with established DMN governance processes High (20)
Operational : Security training or awareness High (16)
Operational : Unauthorised devices on corporate network High (15)
Operational : Unauthorised software installation High (15)
Operational : Medical device safeguards and system maintenance are not consistently completed Medium (12)
Operational : Lack of portfolio, program and project management framework Medium (14)
Operational : System handover to BAU Medium (14)
Operational : Network able workstations in publicly accessible areas Medium (10)
Operational : Cyber security vulnerabilities in server operating system patching backlog (ALARP Low)

KPIs:

1. Report on eHQ control uplifts
2. Report on compliance and new areas undertaking compliance reporting
3. Report on approvals and risks associated with architectural reviews

4.4 Detect

The Detect Function defines the appropriate activities to identify the occurrence of an information security event. The Detect Function enables timely discovery of information security events.

Outcome Categories within this Function include:

- Ensuring Anomalies and Events are detected, and their potential impact is understood (from having a view of what normal looks like)
- Implementing Security Continuous Monitoring capabilities to monitor information security events and verify the effectiveness of protective measures including network and physical activities
- Maintaining Detection Processes to provide awareness of anomalous events

Current state:

- Reliance of eHQ work with limited access and visibility over the tools for MNH

Initiatives / control uplifts / improvements:

4.4.1 Ensure MNHHS has visibility over eHQ detection and monitoring tools (eHQ SIEM, Splunk, Loginsight, McAffee)

4.4.2 Investigate automation of detection software and remediation

4.4.3 Provide reporting and visibility to governance groups

Aligned risks:
Operational : Recognising and reporting Cyber incidents Medium (12)
Operational : Inadequate review of system logs High (15)
Operational : Inadequate User Activity Logging High (16)
Operational : Inadequate System Event Monitoring High (15)

KPIs:

1. Report on eHQ provided detection tools (quarterly)

4.5 Respond

The Respond Function includes appropriate activities to take action regarding a detected information security incident. The Respond Function supports the ability to contain the impact of a potential information security incident.

Outcome Categories within this Function include:

- Ensuring Response Planning process are executed during and after an incident
- Managing Communications during and after an event with stakeholders, law enforcement, external stakeholders as appropriate
- Analysis is conducted to ensure effective response and support recovery activities including forensic analysis, and determining the impact of incidents
- Mitigation activities are performed to prevent expansion of an event and to resolve the incident
- The organization implements Improvements by incorporating lessons learned from current and previous detection / response activities

Current state:

- Incident management procedure in place
- Lack of clarity over improvements, risks or lessons learnt from incidents

Initiatives / control uplifts / improvements:

4.5.1 Centralised reporting eHQ SNOW, CSG service, uplift cyber incident management process

4.5.2 Plan and establish a backup control system to enable communications and backups to continue in case of total loss, plan, map, decision trees, roles and accountability.

4.5.3 Timed backups to assist in ransomware recovery

4.5.4 Communication and awareness

Aligned risks:
Operational : Recognising and reporting Cyber incidents Medium (12)
Operational : DMN provided storage backups to mitigate cryptolocker attacks High (19)
Operational : Inadequate Backup and Recovery High (15)
Operational : Security training or awareness High (16)
Audit action : System Recovery Plans (SRP) have not been approved or tested High
Audit action : Business Impact Analysis (BIA) results are not evidenced High

KPIs:

1. Report on incidents including risk and lessons which come from the incidents
2. Develop a plan for backup with MNHHS EOC

4.6 Recover

The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information security incident. The Recover Function supports timely recovery to normal operations to reduce the impact from an information security incident.

Outcome Categories within this Function include:

- Ensuring the organization implements Recovery Planning processes and procedures to restore systems and/or assets affected by information security incidents
- Implementing Improvements based on lessons learned and reviews of existing strategies
- Internal and external Communications are coordinated during and following the recovery from an information security incident

Current state:

- Backups conducted but not tested
- Limited number of BIL, SRPs completed

Initiatives / control uplifts / improvements:

4.6.1 Establish the BIL, SRP, DR for existing and new services

4.6.2 Ensure appropriate backups

4.6.3 Ensure testing is conducted of backups and restore functions (including data integrity checks)

4.6.4 Obtain same from eHQ and other vendors via assurance or KPIs etc (enterprise wide BCP, DR and SRP, assurance)

Aligned risks:
Operational : DMN provided storage backups to mitigate cryptolocker attacks High (19)
Operational : Inadequate Backup and Recovery High (15)
Organisational : eHQ and HSQ supported systems require assurance and documented escalation path High (16)
Audit action : System Recovery Plans (SRP) have not been approved or tested High

KPIs:

1. Report on progress of completing prioritised BIL, SRP for existing services (minimum 1/mth)
2. Report on backup and restore testing completed (minimum 1/mth)
3. Report on eHQ enterprise BIL, SRPs.

Appendix 1 Acronyms and abbreviations

Term or Acronym	Description
ALARP	As Low as Reasonably Possible
BAU	Business as Usual
BCP	Business Continuity Plan
BIL	Business Impact Level
BTS	Biomedical Technology Services
CDHO	Chief Digital Health Officer
CE	Chief Executive
CFCO	Chief Finance and Corporate Officer
CIA	CIA Triad – Confidentiality, Integrity, Availability
CIM	Clinical Incident Management
CIO	Chief Information Officer
CSG	Cyber Security Group
DCPCG	Digital Clinical Portfolio Control Group (governance)
DMN	Digital Metro North
DoH	Department of Health
DR	Disaster Recovery
DTEC	Digital Transformation Executive Committee
eHQ	eHealth Queensland
EOC	Emergency Operations Centre
GSI	Governance and Strategic Initiatives
HHS	Hospital and Health Service
HIMS	Health Information Management Services
HSD	Health Service Directive
IAMS	Identity Access Management Service
ICT	Information and Communication Technology
ISMS	Information Security Management System
ISRAP	Information Security Risk Assessment Process
KPI	Key Performance Indicator
MNH	Metro North Health
MNHHS	Metro North Hospital and Health Service
MNIMG	Metro North Information Management Group
NIST	National Institute of Standards and Technology
PAM	Privileged Access Management
QG	Queensland Government
QGCDG	Queensland Government Customer and Digital Group
QGCIO	Queensland Government Chief Information Office
QH	Queensland Health
RBWH	Royal Brisbane and Women's Hospital
RG	Research Governance
SAAS	Software as a Service
SNOW	Service Now
SOCI	Security of Critical Infrastructure Act
SoE	Standard Operating Environment
SRP	System Recovery Plan
TPCH	The Prince Charles Hospital

Appendix 2 Definitions

Term	Description
Business Continuity Management	Preparing for and maintaining continued business operations following disruption or crisis.
Cyber attack	A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or prosperity.
Disaster Recovery	Disaster Recovery involves activities to enable efficient and effective recovery of vital technology infrastructure and systems following a natural or human-induced disaster.
Health Data	Health Data is comprised of both personal information and sensitive information. Generally, it includes clinical metrics along with environmental, socioeconomic, and behavioural information pertinent to healthcare.
ICT Asset	All applications and technologies that are owned, procured and/or managed by the agency. These include desktop and productivity tools, application environments, hardware devices and systems software, network and computer accommodation, and management and control tools.
Information	Information is any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, and textual or numerical form.
Medical Data	Medical Data is a ‘Data Set’ and a subset of Health Data. The best-known form is clinical data which is commonly associated with the electronic health record.
Owner	Information as an asset is owned by the State of Queensland. The term owner in the Strategic Direction is the recognised officer who is identified as having the authority and accountability under legislation, regulation or policy for the collection of information assets on behalf of the State of Queensland. Information owners define the policy which governs the information assets of an agency, for example determining the security classification of information assets. An owner will often delegate the operational responsibility for information assets to a custodian, who applies controls that reflect the owner’s expectations and instructions such as ensuring proper quality, security, integrity, correctness, consistency, privacy, confidentiality and accessibility of the information assets.
Penetration testing	A penetration test is an authorized simulated cyberattack on a computer system, application or network performed to evaluate the security of the system.
Privacy Impact Assessment	A Privacy Impact Assessment is a process which assists organizations in identifying and minimizing the privacy risks for solutions.
Risk Appetite	The amount and type of risk that an organisation is willing to pursue or retain in the pursuit of its organisational objectives. The MNHH Board sets and reviews the organisation’s risk appetite (annually)
Risk Assessment	A risk assessment is the combined effort of: identifying and analysing potential events that may negatively impact individuals, assets, and/or the environment; and making judgments "on the tolerability of the risk on the basis of a risk analysis" while considering influencing factors.
Security Incident Management	computer security incident management involves the monitoring and detection of security events on a computer, network or application, and the execution of proper responses to those events.
Shadow IT	The adoption and use of applications/services by employees without the knowledge or approval of the IT department.
Vulnerability	A flaw or weakness that can be used to attack a system or organization.
Vulnerability scanning	A security scanning to assess computers, networks or applications for known weaknesses.

Appendix 3 References and related documents

Document type	Document name	Location
ISMS Manual	Metro North Hospital and Health Service ISMS Manual	MNHHS ISMS Manual v1.02.pdf
Information Security Policies	Information Security Policy (IS18:2018)	Information security policy (IS18:2018) | Queensland Government Enterprise Architecture (qgcio.qld.gov.au)
	Information Security – Digital Policy QH-POL-468:2019	QH Information Security Policy
Policy	Data Custodianship 004570	Policy: Data Custodianship 004570 | Metro North Hospital and Health Service
Procedure	Data Custodian and Application Custodian 005836	Data Custodian and Application Custodian 005836 (health.qld.gov.au)
Procedure	Health Technology (Medical Devices) Management 006174	(Health Technology (Medical Devices) Management 006174)
Organisational Structure	Queensland Health Organisational Structure	Queensland Health organisational structure | Queensland Health
Legislation	Hospital and Health Boards Act 2011	Hospital and Health Boards Act 2011 (legislation.qld.gov.au)
Health Service Directive	Enterprise Information, Communications and Technology (ICT) Governance	Enterprise information, communications and technology (ICT) governance | Health service directive | Queensland Health
Information Security Policies and Standards	ICT Policies	ICT policies | Queensland Health
Framework	ICT Governance Framework	Department of Health Report Publication template
Governance listing	Committees	System ICT Governance committees - eHealth Queensland
Application listing	Enterprise Applications	Queensland Health Applications Index | Queensland Health Intranet
Statement	Risk Appetite Statement	MNHHS risk appetite