



The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38EC(1)(b)(iii) of the *Government Sector Audit Act 1983*, I present a report titled 'Cyber Security in Local Health Districts' to the Houses of Parliament for publication. I additionally present for publication a foreword as addendum to this report.

Please note that on 9 July 2025, I presented this report confidentially under section 38EC(1)(b)(i) of the *Government Sector Audit Act 1983*, including the agency response presented in Appendix 1.

Bola Oyetunji
Auditor-General for New South Wales
19 December 2025

AUDITOR-GENERAL'S FOREWORD

My [Cyber security insights 2025](#) report noted that modern governments' dependence on IT and global network interconnectivity has significantly raised cyber security risks. Incidents such as data theft, privacy breaches, and denial of access to essential systems can disrupt public services and erode trust in government.

The 'Cyber security in Local Health Districts' report was completed in July 2025. I determined that it was not in the public interest to make the report public at that time. As such, I presented the report to Parliament on a confidential basis on 9 July 2025 to be published on 19 December 2025, allowing NSW Health to take action in response to the report recommendations prior to publication.

In the time since presentation of the confidential report, NSW Health has established a taskforce and progressed action in response to the report's recommendations.



NEW SOUTH WALES AUDITOR-GENERAL'S REPORT

Cyber security in Local Health Districts

PERFORMANCE AUDIT | 9 JULY 2025

ROLE OF THE AUDITOR-GENERAL

The roles and responsibilities of the Auditor-General and the Audit Office, are set out in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

We conduct financial or 'attest' audits of state public sector and local government entities' financial statements. We also audit the Consolidated State Financial Statements, a consolidation of all state public sector agencies' financial statements.

Financial audits are designed to give reasonable assurance that financial statements are true and fair, enhancing their value to end users. Also, the existence of such audits provides a constant stimulus to entities to ensure sound financial management.

Following a financial audit the Audit Office issues a variety of reports to entities and reports periodically to Parliament. In combination, these reports give opinions on the truth and fairness of financial statements, and comment on entity internal controls and governance, and compliance with certain laws, regulations and government directives. They may comment on financial prudence, probity and waste, and recommend operational improvements.

We also conduct performance audits. These assess whether the activities of government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws. Audits may cover all or parts of an entity's operations, or consider particular issues across a number of entities. Our performance audits may also extend to activities of non-government entities that receive money or resources, whether directly or indirectly, from or on behalf of government entities for a particular purpose.

As well as financial and performance audits, the Auditor-General carries out special reviews, compliance engagements and audits requested under section 27B(3) of the *Government Sector Audit Act 1983*, and section 421E of the *Local Government Act 1993*.



GPO Box 12
Sydney NSW 2001

The Legislative Assembly
Parliament House
Sydney NSW 2000

The Legislative Council
Parliament House
Sydney NSW 2000

In accordance with section 38EC(1)(b)(i) of the *Government Sector Audit Act 1983*, I present a report titled '**Cyber Security in Local Health Districts**' to the Houses of Parliament on a confidential basis.

A handwritten signature in black ink, which appears to read 'Bola Oyetunji'.

Bola Oyetunji
Auditor-General for New South Wales
9 July 2025

RECONCILIATION STATEMENT

We pay our respects and recognise Aboriginal peoples as the traditional custodians of the land in NSW who have cared for and protected the environment, waterways, and sacred sites over many millennia. We honour and thank the traditional custodians of the land on which our office is located, the Gadigal people of the Eora Nation, and the traditional custodians of all the lands on which our employees live and work. We pay our respects to their Elders past and present, and to the next generation of leaders.

We acknowledge that our long history of helping to foster accountability and transparency in the government and Parliament is also shared with the histories of colonisation and the resulting disadvantage of Aboriginal and Torres Strait Islander peoples in this state.

We embrace our role in holding government agencies to account for the delivery of effective services for Aboriginal and Torres Strait Islander peoples. We are committed to ensuring that our audits are culturally responsive, respectful and inclusive, and that we engage with Aboriginal and Torres Strait Islander peoples and communities in a meaningful and collaborative way.

We recognise the ancestral tie of Aboriginal and Torres Strait Islander peoples to this land, and we acknowledge that we have much to learn from their wisdom, rich and diverse culture, languages, knowledge and practices.

contents

Cyber security in Local Health Districts

1.	Executive Summary	1
	Conclusion	1
2.	Introduction	5
	2.1. The importance of cyber security risk management	5
	2.2. Relevant NSW Health organisations	5
	2.3. Legislative and policy framework for cyber security	6
	2.4. Audit focus	7
3.	Managing cyber security risks to clinical systems	8
	3.1. Cyber security responsibilities and funding	8
	3.2. Identifying vital ICT assets for protection	9
	3.3. Considering threats to ICT assets	9
	3.4. Cyber security culture in Local Health Districts	11
4.	Responding to cyber security attacks	13
	4.1. Cyber security controls	13
	4.2. Monitoring and detecting cyber security incidents	14
	4.3. Preparedness for cyber security attacks	15
	Appendix 1 – Response from entity	17
	Appendix 2 – About the audit	20
	Appendix 3 – Performance auditing	22

1. Executive Summary

Context

The New South Wales (NSW) public health system includes more than 220 public hospitals, community and other public health services. 15 Local Health Districts across NSW administer the hospitals and other health services. eHealth NSW was established in 2014 to provide statewide leadership on the planning, implementation and support of information communication technologies (ICT) and digital capabilities across NSW Health.

Health service delivery is increasingly reliant on digital systems, which in turn requires the effective management of cyber security risks. Cyber attacks can harm health service delivery and may include the theft of information, breaches of private health information, denial of access to critical technology or even the hijacking of systems for profit or malicious intent. These outcomes can adversely affect the community and damage trust in government.

Audit objective

This audit assessed whether NSW Health is effectively safeguarding clinical systems, required to support healthcare delivery in Local Health Districts, from cyber threats. The audit assessed this with the following questions:

1. Do relevant NSW Health organisations effectively manage cyber security risks to clinical systems?
2. Do relevant NSW Health organisations effectively respond to cyber attacks that affect the clinical systems that are essential for service delivery?

To focus the audit, 4 of the 15 Local Health Districts were selected for audit. These districts are referred to as ‘the audited Local Health Districts’ throughout this report. The audit further focused on one facility in each of the audited Local Health Districts that provided a common type of healthcare service. The names of the audited Local Health Districts, selected facilities and healthcare services are not disclosed.

Conclusion

NSW Health is not effectively managing cyber security risks to clinical systems that support healthcare delivery in Local Health Districts. In addition, Local Health Districts have not met the minimum NSW Government cyber security requirements that have been outlined in NSW Cyber Security Policy since 2019.

Local Health Districts are not adequately prepared to respond effectively to cyber security incidents. Systemic non-compliance with NSW Government cyber security requirements, including maintaining adequate cyber security response plans, business continuity planning and disaster recovery for cyber security incidents, means that Local Health Districts could not demonstrate that they are prepared for, or resilient to, cyber threats. This exposes the risk that a preventable cyber security incident could disrupt access to healthcare services and compromise the security of sensitive patient information.

eHealth NSW has not clearly defined or communicated its roles and the expected roles of Local Health Districts regarding cyber security. This has led to confusion amongst Local Health Districts on the cyber security risks they manage, including for crown jewel assets (the ICT assets regarded as valuable or operationally vital for service delivery), and identifying and mitigating critical vulnerabilities, threats and risks. Local Health District management of cyber security is hampered by a lack of support, coordination and oversight from eHealth NSW in cyber security matters.

Key findings

Local Health Districts do not manage cyber security risks effectively

Local Health Districts generate, use and maintain large volumes of sensitive personal and health information about patients. The NSW Cyber Security Policy sets out an expectation that cyber security efforts are commensurate with the potential effect of a successful cyber breach. Under NSW Health policy, Local Health Districts, in collaboration with eHealth NSW, are responsible for managing cyber security and resourcing a fit-for-purpose cyber security function. The current NSW Cyber Security Policy 2023–2024 recognises that agencies providing critical or high-risk services, such as Local Health Districts, should implement a wider range of controls and aim for broader coverage and effective implementation of additional controls.

However, the audited Local Health Districts have not complied with the minimum requirements of the NSW Cyber Security Policy since it was introduced in 2019. None of the four districts had effective cyber security plans. Local Health Districts that do not have effective cyber security plans cannot articulate their approach to managing cyber security risks and are not adequately prepared to respond to and manage cyber security risks and incidents.

Local Health Districts do not have plans and processes in place to respond effectively to a cyber attack

None of the audited Local Health Districts had effective cyber security response plans. Nor did Local Health District business continuity plans and disaster recovery plans consider cyber security risks. Local Health Districts that do not have effective cyber security response, disaster recovery or business continuity plans that include considerations of cyber security, may not be able to safeguard clinical systems against potential cyber security incidents. This may also hamper responses during an incident because roles and responsibilities may not be understood, and actions to address cyber security incidents may not be undertaken as quickly as required, affecting the delivery of services to patients.

NSW Health has not clearly communicated cyber security roles and responsibilities amongst NSW Health organisations

eHealth NSW coordinates cyber security matters within NSW Health. However, eHealth NSW has not clearly defined and communicated its roles and the expected roles of Local Health Districts for cyber security. This has led to confusion amongst Local Health Districts on the cyber security risks they manage, including for crown jewel assets (the ICT assets regarded as valuable or operationally vital for service delivery) and identifying and mitigating critical vulnerabilities, threats and risks.

eHealth NSW does not provide Local Health Districts with sufficient support to manage cyber security risks, and Local Health Districts have not applied the tools provided by eHealth NSW to all clinically important systems

eHealth NSW has developed and distributed cyber security frameworks, guidance and training to all Local Health Districts. eHealth NSW has developed whole-of-system tools to meet key requirements of the NSW Cyber Security Policy and improve the effectiveness of Local Health Districts' cyber security activities. These tools include risk assessment frameworks. However, eHealth NSW has not ensured that its tools have been implemented in Local Health Districts, nor whether Local Health Districts have the capability or capacity to do so.

In the audited Local Health Districts, the effectiveness of eHealth's cyber threat identification tools is hampered by incomplete application to all clinically important ICT assets. This means that critical systems used by Local Health Districts to deliver, or support the delivery of, clinical treatment are not effectively protected from cyber security incidents.

Local Health Districts do not have an effective cyber security culture

In all audited Local Health Districts, critical cyber security controls are not consistently applied by clinical staff who perceive a tension between the urgency of clinical service delivery and the importance of cyber security policies. This has led to normalisation of non-compliance with cyber security controls. This audit observed clinical staff non-compliance at all audited Local Health Districts with multiple cyber security controls that Local Health Districts had put in place.

Despite known systemic non-compliance by clinical staff, the audited Local Health Districts have not assessed the effectiveness of the controls they have put in place, nor have they identified any alternatives that might balance the need for clinical urgency with effective cyber security practice. In addition, they have not considered investing in alternative ICT solutions that better meet the needs of clinical staff while also addressing cyber security concerns.

NSW Health's Cyber Security Policy attestation lacks transparency on the level of cyber security capability within the health system

The NSW Cyber Security Policy requires an agency head to attest to the agency's compliance with the policy. In 2023, eHealth NSW surveyed all NSW Health organisations, including Local Health Districts, on their self-assessed maturity against the NSW Cyber Security Policy in developing a summary assessment for NSW Health to inform its attestation of NSW Cyber Security Policy compliance. That summary showed that Local Health Districts had immature cyber security controls, including for the Essential Eight controls – the most effective set of controls identified by the Australian Cyber Security Centre.

However, in 2024, the survey was not completed, so NSW Health aggregated its assessment of whether NSW Health organisations had met NSW Cyber Security Policy requirements. This audit identified systemic Local Health District non-compliance with NSW Cyber Security Policy. The 2024 attestation therefore obscures the risks that exist in Local Health Districts. If NSW Health continues to attest to Cyber Security Policy compliance in the aggregate, the risk is that neither NSW Health nor Cyber Security NSW fully understand where and what the cyber security risks are across NSW Health organisations.

Recommendations

The Ministry of Health should:

1. by October 2025, collate and validate information on compliance with NSW Cyber Security Policy by each entity that reports to or via the Ministry of Health prior to annual attestation
2. by December 2025, finalise and communicate cyber security roles and responsibilities within the NSW Health system.

By December 2025, eHealth NSW should:

3. work with the Ministry of Health to develop clear guidance for Local Health Districts on the obligation to manage the need to deliver clinical services while meeting critical cyber security requirements
4. determine and apply sufficient resources to support the Privacy and Security Assessment Framework and Cyber Security Risk Assessments in Local Health Districts
5. support Local Health Districts to improve cyber security capability by
 - a) articulating a whole-of-health cyber security risk appetite statement
 - b) providing direct assistance to localise centrally developed tools and frameworks
 - c) ensuring all Local Health District crown jewel assets are monitored by the Health Security Operations Centre.

By December 2025, Local Health Districts should:

6. design and implement a fit-for-purpose cyber security risk management framework incorporating:
 - a) an enterprise cyber security risk appetite statement, which aligns with the whole-of-health statement
 - b) complete up-to-date cyber security and cyber security response plans, which are regularly tested and updated
 - c) investment in establishing and maintaining the Essential Eight cyber controls
 - d) cyber security controls that identify and address the root causes of non-compliance and balance the need for clinical urgency with effective cyber security
 - e) consideration of cyber security needs in the implementation of any new clinical systems.

2. Introduction

2.1. The importance of cyber security risk management

Increasing digitisation of healthcare related information and systems has increased the risk of cyber security threats over time. NSW Health handles and manages sensitive information. In healthcare settings, there are numerous types of sensitive information that could be attacked for financial gain. Potential targets of cyber security attacks and breaches could include personal health information, research information and web-enabled medical devices. This information can be found in government systems as well as third-party applications. NSW Health reports that healthcare is the most breached industry in Australia, and health data is 50 times more valuable than credit card data on the dark web.

In 2020, as part of a business case for additional investment in cyber security, NSW Health reported that it analysed 58 billion activity and systems logs each month. This included 401,000 security events across 2019–2020, and 41,419 events validated as cyber security incidents that were investigated and responded to. The effects of cyber security incidents across NSW Health could be significant.

2.2. Relevant NSW Health organisations

Ministry of Health

The Ministry of Health supports the executive and statutory roles of the Health Ministers and is led by the NSW Health Secretary. The Ministry of Health undertakes regulatory functions, public health functions and public health system manager functions in statewide planning, purchasing and performance monitoring and support of health services, including the Local Health Districts.

eHealth NSW

eHealth NSW provides statewide leadership on the design, delivery and management of ICT-led healthcare. It is one of several organisations set up under the Health Administration Corporation to provide shared support services to the health system. eHealth NSW partners with Local Health Districts and other NSW Health organisations by managing and supporting enterprise-wide information and communication technology (ICT) systems. In collaboration with Cyber Security NSW, eHealth NSW manages the central cyber security functions of NSW Health. eHealth NSW's Chief Executive is the NSW Health Chief Information Officer. eHealth NSW also supplies the NSW Health Chief Information Security Officer.

Local Health Districts

Local Health Districts manage public hospitals and health facilities and are responsible for providing health services in a wide range of settings across NSW. There are 15 Local Health Districts across NSW, all of which use a vast number of ICT to facilitate the delivery of essential health services. Local Health Districts are separate, board-governed statutory corporations but are subject to governance, oversight and control by the Secretary of NSW Health. Under NSW Health policy, and in collaboration with eHealth NSW, Local Health Districts are responsible for managing cyber security and resourcing a fit-for-purpose cyber security function.

2.3. Legislative and policy framework for cyber security

NSW Cyber Security Policy

Cyber Security NSW is responsible for developing the NSW Cyber Security Policy, which sets out mandatory requirements for NSW Government agencies to ensure that cyber security risks to their information and systems are properly managed. Each year, NSW Government agencies are required to self-assess against the NSW Cyber Security Policy and report that assessment to Cyber Security NSW. In the past this has included a maturity assessment. The most recent policy, issued in February 2024, requires agencies to report whether they have achieved policy requirements. For the first attestation round in October 2024, agencies were asked to submit a baseline assessment of compliance with mandatory requirements.

The NSW Cyber Security Policy recognises that ‘agencies that provide critical or higher-risk services and hold higher-risk information should implement a wider range of controls and aim for broader coverage and effective implementation of those controls’. This guidance is relevant to Local Health Districts due to the critical nature of healthcare services, as well as the private and sensitive nature of the information held by Local Health Districts.

Key requirements of the NSW Cyber Security Policy, since its introduction in 2019, include identification of crown jewel systems (the most valuable and operationally vital systems or information in an organisation), cyber security considerations in business continuity and disaster recovery planning, and implementation of the Essential Eight cyber controls. The Essential Eight cyber controls were developed by an Australian Government agency, the Australian Cyber Security Centre, in 2017. The Australian Cyber Security Centre identified the Essential Eight model as the most effective set of controls. An entity implementing these controls would be well placed to protect itself from many cyber threats. The Essential Eight controls are:

1. patch applications
2. patch operating systems
3. implement multi-factor authentication
4. restrict administration privileges
5. implement application control
6. securely configure Microsoft Office macro settings
7. implement user application hardening
8. maintain backups of important data, software and configuration settings.

Other cyber security risk management guidance and frameworks

Other sources of good practice may inform approaches to identifying and managing cyber security risks. These include Australian Cyber Security Centre resources, the US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity, and relevant Australian and International Organization for Standardization standards, including ISO 27001 Information Security, Cybersecurity and Privacy Protection.

NSW privacy law

Under NSW privacy laws, Local Health Districts are legally obliged to protect the security of personal and health information. Personal information is information about an individual whose identity is apparent or can reasonably be ascertained from the information. Health information is a specific type of personal information that includes information about physical or mental health or disability.

The *Privacy and Personal Information Protection Act 1998 (NSW)* and the *Health Records and Information Privacy Act 2002 (NSW)* require that Local Health Districts holding personal or health information must ensure that the information is protected by taking such security safeguards as are reasonable in the circumstances against loss, unauthorised use, modification or disclosure and against all other misuse. The legislation also requires that Local Health Districts ensure information is kept no longer than necessary, disposed of securely and that organisations act reasonably within their power to ensure that when sharing information, they prevent unauthorised use or disclosure of personal or health information.

Australian critical infrastructure law

The *Security of Critical Infrastructure Act 2018 (Cth)* (the SOCI Act) aims to provide a framework to protect critical infrastructure from risks, including cyber security risks. The SOCI Act designates several NSW hospitals as critical hospital infrastructure assets. This means that NSW Health and the Local Health Districts that operate the hospitals are required to comply with cyber risk management policies set out in the SOCI Act. Regarding cyber security, this includes achieving a minimum level of cyber security controls and incident reporting.

2.4. Audit focus

This performance audit is concerned with whether NSW Health effectively safeguards the clinical systems that are required to support healthcare delivery in Local Health Districts from cyber threats. As a result, the audit focused on assessing the performance of four Local Health Districts through the lens of one selected critical clinical service which is delivered at four hospital facilities within those Local Health Districts. See Appendix 2 for more information about the selection of the clinical service and Local Health Districts.

The audited clinical service, hospital facilities and Local Health Districts remain confidential so that risks, vulnerabilities and challenges can be identified and described within this audit report without placing the audited Local Health Districts at increased risk of a targeted cyber attack. This audit also considers whole-of-system planning, information sharing, guidance, support and performance monitoring of cyber security practices within the Ministry of Health and eHealth NSW.

3. Managing cyber security risks to clinical systems

Clinical systems are required to deliver health services to people presenting to hospitals, community health services and other health services. Disruptions to clinical services caused by cyber attacks can disrupt the delivery of health services. This audit focused on one area of clinical service delivery in four Local Health Districts to understand how effectively the districts manage cyber security risks to the clinical systems used for that area of clinical service delivery.

This chapter looks at how roles and responsibilities relating to cyber security are defined in NSW Health. It examines funding for cyber security activities, considers how Local Health Districts identify the information and communication technology (ICT) assets that require protection, and assesses how Local Health Districts understand the vulnerabilities of clinical systems to cyber threats. It also considers whether Local Health Districts have built and maintained a strong culture of cyber security. This is important because most cyber security attacks are the result of people-related factors rather than technical weaknesses.

3.1. Cyber security responsibilities and funding

Cyber security roles and responsibilities between eHealth NSW and Local Health Districts are not clearly understood

In 2024, eHealth NSW developed a cyber security roles and responsibility framework, which replaced a process whereby individual memoranda of understanding were signed with Local Health Districts. eHealth NSW expects to continuously update the framework as new cyber security requirements and processes emerge rather than at set intervals. In April 2024, an early draft of the framework was circulated to Local Health District Chief Information Officers for comment. In January 2025, the document was published on the NSW Health intranet.

The cyber security roles and responsibility framework sets out the responsibilities of eHealth NSW and Local Health Districts against the mandatory requirements of the NSW Cyber Security Policy and implementation of the Essential Eight controls. The framework outlines how eHealth NSW can help Local Health Districts meet requirements by listing eHealth NSW products and services that are available to NSW Health organisations to procure. It also provides relevant resource links. The framework does not set out eHealth NSW's responsibilities for cyber security that exist outside of its relationship to Local Health Districts. In this way the framework is not a complete description of cyber security roles and responsibilities in NSW Health.

When interviewed as part of this audit, cyber security staff at the four audited Local Health Districts expressed varying levels of confusion about the role of eHealth NSW and were unaware of the development and position of the framework. There is an opportunity for eHealth NSW to better communicate the framework to ensure that cyber security gaps and vulnerabilities are not exposed due to a lack of understanding of roles and responsibilities.

Neither eHealth NSW nor Local Health Districts meet cyber security benchmark spending

A December 2024 NSW Government review of cyber security expenditure determined that an appropriate benchmark for NSW public sector cyber security expenses as a proportion of ICT expenses was nine per cent. Moreover, eHealth NSW reported that it spent \$27.9 million on cyber security in 2023–24 or 2.15% of ICT expenses. Moreover, 35 full-time equivalent staff were employed in the cyber security area in this period. This complements significant contractor and consultant spending on cyber security.

Most Local Health Districts in NSW reported to the review that they have one full-time equivalent staff member dedicated to cyber security. However, some larger districts have more staff in this area and a few Local Health Districts share cyber security resources. Local Health Districts spent on average \$421,000 on cyber security in 2023–24 or about two per cent of ICT expenses.

3.2. Identifying vital ICT assets for protection

Most audited Local Health Districts consider the clinical importance of ICT assets when identifying crown jewels

Since the creation of the NSW Cyber Security Policy in 2019, NSW Government agencies have been required to assess and identify crown jewels and classify systems according to risk and importance. Crown jewel systems are the most valuable and operationally vital systems or information in an organisation, and identifying them highlights their importance so that ICT staff can ensure that they are included and protected as part of cyber security management activities. eHealth NSW developed a Crown Jewel Framework to help Local Health Districts identify crown jewel systems.

The framework includes considerations of clinical importance and the use of the ICT asset across, and its impact on, the NSW Health system. However, eHealth NSW has not mandated the use of the framework, nor does it validate Local Health District use of the framework. eHealth NSW's decision not to require Local Health Districts to utilise its framework raises the risk that Local Health Districts may not appropriately identify crown jewels, which could put them in breach of the policy and put their ICT assets at increased risk.

eHealth NSW used this framework to identify 41 crown jewels for the whole of NSW Health, which includes two clinical systems it has identified as the responsibility of Local Health Districts. Each of the audited Local Health Districts has also identified these latter systems as crown jewels. Three of the four Local Health Districts included in this audit used eHealth's Crown Jewel Framework to guide their identification of local crown jewel systems and considered clinical importance as part of their assessments. However, the other Local Health District did not utilise the framework to identify its crown jewels, because it assessed and identified crown jewel systems in 2021, before the framework had been created.

3.3. Considering threats to ICT assets

Audited Local Health Districts' cyber threat intelligence monitoring systems provide them with an understanding of known system vulnerabilities

The audited Local Health Districts monitor threats and vulnerabilities via subscription service updates that are generated by eHealth NSW, Cyber Security NSW, the Australian Government, and system and application vendors.

This allows them visibility over missing patches or updates across ICT systems and applications, which can create opportunities for cyber attacks or incidents unless the missing patch or update is applied.

Audited Local Health Districts could not demonstrate that patches and updates to clinical systems are timely nor informed by anticipated effects on clinical service delivery

ICT staff at the audited Local Health Districts report that they work to ensure that they apply patches and updates to clinical systems in a way that does not affect clinical service delivery. This is appropriate to minimise downtime during hours when patients are being treated.

However, because ICT teams need to wait for a clinically appropriate time to apply system patches and updates, there is a risk that those systems may be vulnerable to the threats that the updates and patches are intended to address. This could result in attackers taking advantage of a known vulnerability to gain access to Local Health District ICT assets during the window of time between the vulnerability being identified, and its immediate resolution outside of clinical service delivery hours. Audited Local Health Districts could not demonstrate a patching routine or how that routine considered clinical service delivery.

Most audited Local Health Districts use vulnerability and incident identification products designed to protect ICT assets from cyber security threats

Local Health Districts can access several products that are designed to protect and provide cyber security for their ICT assets, including the Health Security Operations Centre and off-the-shelf products mandated for use. Cyber attacks on unprotected clinical systems could compromise the availability of clinical systems, records tampering and other outcomes that could harm patients.

As required by NSW Health policy, most of the audited Local Health Districts use these products, but other Local Health Districts were unable to demonstrate that they used these tools consistently. eHealth NSW does not have direct visibility over which Local Health Districts use these tools and for which ICT assets. eHealth NSW uses these tools for NSW Health Crown Jewel Assets.

Local Health Districts do not consistently assess new or existing ICT assets for security threats

In 2015 eHealth NSW established the Privacy and Security Risk Assessment Framework (PSAF) to address cyber security policy requirements. eHealth NSW provides the assessment, which identifies security and privacy threats during an ICT project and assists with the establishment of appropriate security controls to safeguard information assets. The PSAF is not mandatory, but eHealth NSW recommends Local Health Districts use it for all ICT system procurement and major updates.

There are many legacy ICT systems in the NSW Health network. For this reason, eHealth NSW recommends that Local Health Districts also consider applying the PSAF to legacy systems that were implemented prior to the creation of the PSAF. ICT assets that do not undergo this assessment may be more exposed to threats and may not have appropriate plans in place to address cyber security risks.

The audited Local Health Districts do not undertake PSAF assessments for all new procurements or updates and have not assessed their legacy ICT systems. This raises the risk that Local Health Districts do not understand and may not implement appropriate controls for these ICT systems. Consequently, these ICT assets may be more vulnerable to cyber attack.

In the last three years, the audited Local Health Districts have completed at least 15 PSAFs and, as of April 2025, were waiting for a further eight PSAFs. They have not applied the PSAF to the many legacy systems they operate. While the Local Health Districts find the PSAF process useful, the main barriers to using it more regularly are:

- the high cost of undertaking the PSAF process, with costs between \$4,550 and \$30,000 and up to \$60,000 with additional testing
- the considerable time it takes to complete the process (one audited Local Health District reported that a PSAF request was open with eHealth NSW for almost a year before support was provided).

eHealth NSW created the Cyber Security Risk Assessment for Local Health Districts without assessing their capability to conduct the assessments

In 2023, eHealth NSW implemented the Cyber Security Risk Assessment to address Local Health Districts commissioning variable and less comprehensive security assessments than the PSAF. It was also intended to be a less intensive assessment for smaller or less critical ICT assets that do not require a PSAF assessment according to an eHealth NSW-administered risk assessment.

The Cyber Security Risk Assessment is undertaken by local ICT staff within Local Health Districts. eHealth NSW does not provide support or validate the work of these staff. One of the four audited Local Health District reports that it is not using the Cyber Security Risk Assessment as it considers it a draft tool. The remaining three districts provided limited evidence that they use the Cyber Security Risk Assessment. Additional validation and any resulting calibration of the Cyber Security Risk Assessment by eHealth NSW would help ensure that there is consistency in practice across Local Health Districts and help ensure that there are adequate cyber security controls in place consistent with risk. Local Health Districts that do not undertake a PSAF or a Cyber Security Risk Assessment are not assessing their ICT assets for cyber security threats.

3.4. Cyber security culture in Local Health Districts

Clinical staff in Local Health Districts frequently disregard cyber security controls, and audited Local Health Districts have not addressed non-compliance

Local Health Districts operate within a culture of clinical urgency, where the time critical treatment of patients takes precedence. This has led to normalisation of non-compliance with cyber security controls. The Audit Office identified systemic non-compliance with cyber security controls consistently across the audited Local Health Districts. Exhibit 1 contains Audit Office observations of non-compliance with cyber security controls.

Exhibit 1: Observed and reported non-compliance with cyber security controls

Uploading, saving or storing patient information outside of secure systems and applications: ICT staff at the audited Local Health Districts advised that, despite implementing rules for clinicians not to save and host patient information on their own devices outside of clinical systems, clinicians often did so. Further, some clinicians uploaded patient information to unsecured systems and applications. Although both clinical and ICT staff at Local Health Districts acknowledge that clinicians engaging in this practice do so to facilitate the delivery of clinical services to patients, hosting private patient information and data outside of secure authorised environments makes a cyber security incident or attack much more likely to occur. Local Health District ICT staff advised that it is difficult to raise this issue directly with the clinical staff engaging in these practices because of siloed environments and management structures between clinical and operational staff, and a lack of understanding of the risks involved.

Lack of secure solutions for information sharing between Local Health District clinical services and other healthcare providers, such as general practitioners: Clinicians at the audited Local Health Districts use outdated communication tools (such as fax machines) to provide and receive patient referrals and share patient information. Moreover, fax is often the only secure option for referring doctors to provide referrals, as emails are not a secure method to send or receive private patient information. However, clinical staff also report that they use emails to share patient information because there is a lack of other options to share information with other clinicians or provide information directly to patients.

Leaving computers 'logged in' when unattended: For clinical staff, who move between clinical spaces and use multiple systems while providing services to patients, logging in and out of computers and devices is a frequent requirement. Clinical staff can be logging in and out of devices and systems several times in a short period of time. This is cumbersome and disruptive because it interrupts their clinical processes and forces them to stop and re-start their tasks. Additionally, audited Local Health District staff reported that some clinical systems can be slow and require long and complicated passwords that can add even more time to the process of logging in and out of systems while providing clinical care. As a result, staff regularly do not log out of systems.

Source: Audit Office of New South Wales fieldwork in Local Health Districts.

Consistent with broader industry experience, ICT staff in the audited Local Health Districts reported that the human element, such as mistakes or non-compliant behaviour, is a more concerning and challenging cyber security risk than any of the other risks they face in maintaining effective cyber security. Despite being aware of clinical staff's systemic non-compliance with cyber security controls, the audited Local Health Districts have not undertaken work to assess the effectiveness of the controls, nor have they investigated alternatives that may balance the need for clinical urgency with effective cyber security. For example, some Local Health Districts in NSW have attempted to address the issue of leaving computers logged in while unattended by providing log-ins to computers via physical access cards, which can be swiped to log in to a computer.

Local Health Districts could do more to resource, plan, and implement systems and practices that address the clinical environment, and support and enable clinical staff to deliver healthcare services in a way that does not compromise cyber security.

Annual cyber security awareness training is mandatory for all NSW Health employees

As of October 2024, all NSW Health staff must complete annual mandatory cyber security training. Previously, following the launch of the training in 2021, staff were required to complete the mandatory training every two years. In April 2025, most Local Health Districts achieved mandatory cyber security training completion rates over 70% against a statewide benchmark of 85%.

In 2024, eHealth NSW developed cyber security awareness materials. The audited Local Health Districts use this material to encourage staff to complete mandatory training, comply with cyber security policies, provide cyber security tips, and notify staff about workshops and lunch and learn sessions. eHealth NSW has not evaluated the use of cyber security materials.

Local Health Districts embed a systems administrator to provide technical support for crown jewel ICT systems, but roles and responsibilities are not always clear

In all the audited Local Health Districts, technical systems administrators are embedded within a clinical service area that utilises a crown jewel ICT system to facilitate clinical service delivery. The embedded systems' administrators provide direct support to the crown jewel ICT system. However, they do not focus on cyber security needs and requirements. Further, the lines of responsibility between embedded staff and Local Health District ICT teams are not formalised.

Local Health Districts that do not have formal arrangements between their ICT teams and specialist ICT embedded staff are vulnerable to governance and cyber security-related risks. Without formal arrangements, it is not clear how or whether the crown jewel system is protected against cyber security threats, or who is responsible for responding to incidents relating to this system. Additionally, in the absence of documented and agreed expectations for information sharing, embedded staff may be operating outside of approved or appropriate ICT and cyber security policies.

Cyber security reporting to Local Health District executives focuses on technical compliance activities and does not report all key risks

The audited Local Health Districts do not consistently or sufficiently report to their board or executives on their cyber security performance and progress. Only one audited Local Health District provided evidence of regular and thorough reporting to executives. The remaining three report on their progress in implementing the Essential Eight mitigation strategies. However, their audience and the level of detail surrounding reporting on other cyber security-related activities varied.

None of the audited Local Health Districts reported on the risk relating to clinical staff non-compliance with cyber security controls identified in Exhibit 1. In other words, executives do not receive information about key risk areas relating to cyber security and therefore do not have the ability to mitigate such risks, or to make informed decisions about cyber security, including resourcing, procurement and risk management.

4. Responding to cyber security attacks

This chapter reports on whether Local Health Districts respond to cyber attacks effectively. First, it considers the strength of cyber security controls in Local Health Districts and their capacity to implement them. Second, the chapter looks at how Local Health Districts monitor and detect cyber security incidents. Finally, it considers how well Local Health Districts plan for a cyber security incident. This is essential to ensure that if a cyber security incident does occur, the Local Health District is able to either continue delivering services or that any downtime that results from the incident is minimised.

4.1. Cyber security controls

None of the audited Local Health Districts demonstrated consideration and implementation of cyber controls beyond the minimum requirements for NSW Government agencies

As of 2019, the NSW Cyber Security Policy has required NSW Government entities to define, establish, implement and maintain controls across various information and communication technology (ICT) assets to protect them from cyber threats. In October 2023, as part of the attestation process under the 2021–2022 NSW Cyber Security Policy, the audited Local Health Districts reported to eHealth NSW and to Cyber Security NSW a low level of maturity implementation of the Essential Eight controls and other policy requirements. The audited Local Health Districts did not make an assessment against the 2023–2024 Cyber Security Policy, which requires implementation of the Essential Eight cyber controls.

NSW Health received \$15.96 million over the three years to December 2025 for its Essential Eight uplift program. The funding is targeted towards lifting cyber security maturity against the Essential Eight for NSW Health’s crown jewel systems. NSW Health determined that the money received was not sufficient to fund maturity uplift of crown jewels identified by Local Health Districts and other NSW Health organisations that were not also identified by eHealth NSW. Instead, eHealth NSW provided Local Health Districts with case studies and generic tools developed for the NSW Health uplift program to assist Local Health Districts complete their own uplift programs using existing funds.

The audit found limited evidence that the audited Local Health Districts considered and implemented controls beyond the Essential Eight since the October 2023 assessment. The NSW Cyber Security Policy recognises that ‘agencies that provide critical or higher-risk services and hold higher-risk information should implement a wider range of controls and aim for broader coverage and effective implementation of those controls’. Given that Local Health Districts hold large volumes of personal and health information, this implementation of cyber controls is insufficient.

NSW Health risks non-compliance with federal cyber security requirements

The *Security of Critical Infrastructure Act 2018 (Cth)* (the SOCI Act) aims to provide a framework to protect critical infrastructure from risks, including cyber security risks. Several hospitals in NSW are designated critical hospitals for the purpose of the SOCI Act. Consequently, Local Health Districts and NSW Health more broadly are required to meet risk management and reporting requirements under the SOCI Act.

However, as with the NSW Cyber Security Policy, not all SOCI requirements are enforced as affected entities work to improve cyber security. eHealth NSW reports that it is currently unable to meet SOCI Act requirements and will not be able to comply with the requirements when they are enforced in the future without further action and investment.

NSW Health attested to the NSW Cyber Security Policy requirements in 2024 without validating the accuracy of Local Health District responses

The NSW Cyber Security Policy requires an agency head to attest to the agency's compliance with the policy. In 2023, eHealth NSW surveyed all NSW Health organisations, including Local Health Districts, on their self-assessed maturity against the NSW Cyber Security Policy in developing a summary assessment for NSW Health. However, this was not done in 2024 for the baseline assessment of whether NSW Health met the requirements of the latest version of the Cyber Security Policy.

This audit identified Local Health District non-compliance with NSW Cyber Security Policy. The October 2024 NSW Health attestation provides an aggregate assessment of whether it has met, partially met or not met mandatory requirements of the 2024 Cyber Security Policy across the 32 NSW Health organisations, including the 15 Local Health Districts. The attestation obscures the cyber security risks that exist for each Local Health District. As a result, NSW Health and Cyber Security NSW may not fully understand cyber security risk in this part of the health system, and decision-makers may not fully understand NSW Health's cyber security needs or risks around resource allocation decisions. eHealth NSW proposes taking this same approach for NSW Health's 2025 attestation.

4.2. Monitoring and detecting cyber security incidents

The audited Local Health Districts rely on the Health Security Operations Centre to monitor and detect potential cyber security incidents, but they do not use the Centre to monitor all of their crown jewel assets

Since 2016, the Health Security Operations Centre has constantly monitored threat intelligence for NSW Health systems. Local Health Districts upload logs from systems, applications and devices to the Health Security Operations Centre, which analyses the logs to detect potential cyber security incidents. Once the Centre identifies a potential cyber security incident, it generates an alert for investigation and response. Local Health District staff then investigate the incident, determining whether the Health Security Operations Centre has identified an actual threat for response and action, or if it is a false alarm.

The audited Local Health Districts do not supply all of their crown jewel ICT asset logs to the Health Security Operations Centre. Thus some crown jewel systems do not receive the same level of monitoring as other important health systems. This increases the risk of a successful cyber attack that could affect clinical service delivery.

eHealth NSW does not formally monitor whether the Health Security Operations Centre meets notification and triage performance requirements, but reports that it has not identified any major incidents that the Health Security Operations Centre failed to flag for further investigation.

The time it takes for the Health Security Operations Centre to resolve potential cyber incidents has doubled since January 2024

The Health Security Operations Centre records the time it takes for Local Health Districts to resolve potential cyber incidents. From 1 January 2024 to 28 February 2025, the average time taken by Local Health District and eHealth NSW teams to resolve potential cyber incidents has approximately doubled. This creates the risk that Local Health Districts are not addressing threats in a timely way to reduce exposure to cyber threats and incidents. During the same period the number of potential cyber incidents rated high or critical remained stable and were a small proportion of the incidents investigated by the Health Security Operations Centre. In addition, the number of cyber incidents remained stable overall.

4.3. Preparedness for cyber security attacks

Three of the four audited Local Health Districts do not have a cyber security plan

Since 2021, NSW cyber security policies have required NSW Government agencies to develop a cyber security plan or strategy. Such a plan should describe an organisation's principles, objectives and priorities for cyber security. It should set out how organisations intend to approach the management of cyber security risks, and how they will identify and manage them.

None of the audited Local Health Districts has a complete cyber security plan. One Local Health District has an incomplete plan. The remaining audited Local Health Districts do not have a cyber security plan at all. Without a cyber security plan, Local Health Districts cannot demonstrate how they are prepared for and will manage cyber security risks, who is responsible for managing cyber security incidents, and the risks and threats to their ICT assets. The audited Local Health Districts are not adequately prepared for cyber security incidents.

Audited Local Health District cyber security response plans are outdated, of poor quality and not fit-for-purpose

The Cyber Security Policy requires NSW Government agencies to maintain a cyber incident response plan. Cyber incident response plans identify how entities will respond to cyber security incidents. Three of the four audited Local Health Districts have a cyber security incident response plan. One is currently yet to finalise a cyber security incident response plan.

The audited Local Health Districts' cyber security incident response plans are of low quality because they are not clear on escalation procedures, they include out-of-date details and they do not contain plans to test the cyber security response plan using real-world scenarios. Additionally, audited Local Health Districts have not developed incident response playbooks that describe the actions staff should take to respond to specific types of cyber security incidents, as well as assigning roles and responsibilities for response.

The risk of low-quality cyber security plans is that Local Health Districts may not be prepared for cyber security incidents and will not be able to respond effectively in the event that they do happen. Without further action, this could mean longer than expected unavailability of clinical services.

Half of the audited Local Health Districts do not test their cyber security response plans, or develop playbooks to assign roles, responsibilities and actions to respond to cyber security incidents

Two of the four audited Local Health Districts tested their cyber security response plans in the last three years. The lack of relevant, regularly tested and updated plans is a critical gap in Local Health District cyber security defences. In other words, audited Local Health Districts are not testing their capabilities, or the strength of their planned responses to cyber security incidents, by simulating a cyber incident to understand how they can learn and improve to ensure effective responses to cyber security incidents.

Without regular testing, audited Local Health Districts do not know how robust their cyber security plans are. Consequently, Local Health Districts risk more negative and longer-lasting effects from cyber security incidents.

eHealth NSW conducted its first ever test of the overall NSW Health cyber security incident response plan in late 2024, but it did not include sufficient clinical involvement, nor test for likely scenarios such as a direct attack on a clinical service

In October 2024, eHealth NSW conducted a desktop exercise to test the overall NSW Health cyber security incident response plan. This was the first time NSW Health had tested its response plan. Regular testing of cyber security incident response plans helps ensure that organisations are adequately prepared for a real cyber security incident. The NSW Cyber Security Policy requires that these exercises are conducted at least annually. eHealth NSW scoped the October 2024 test to focus on coordination between the Ministry of Health, eHealth NSW and NSW Health organisations, including Local Health Districts. The test scenario involved a data breach of a third party platform, including administrative and patient information.

The post-exercise report found that there was room for improvement in how Local Health Districts coordinate with the Ministry of Health and eHealth NSW. For example, eHealth NSW did not provide the incident response playbooks and business continuity plan templates it had developed to Local Health Districts, leading to the inconsistent application of response processes. The report recommended eHealth NSW distribute its incident response templates to standardise and improve response procedures across NSW Health. It also made additional recommendations, including improving communication and role clarification, but there is no established mechanism to accept and then report back on recommendations from the exercise.

Participants in the October 2024 exercise included chief information officers, cyber security specialists and technicians. Clinicians did not participate in the exercise and were not consulted on the findings or recommendations resulting from the exercise. This is an important gap, because while the participants should have a good understanding of health systems, clinicians can provide crucial validation of whether and to what extent the desktop exercise scenario might affect patient health and care. For the scenario tested – a data breach involving a third-party cloud platform – the absence of clinicians was appropriate. However, this low-stakes scenario that did not involve any potential direct consequences for patient care means that the robustness of the NSW Health cyber security incident plan has not been tested sufficiently with scenarios that could have significant detrimental effects on the community.

Audited Local Health District disaster recovery planning and business continuity planning activities do not consider the impacts of cyber security incidents

NSW Health policies require Local Health Districts to prepare a business continuity plan. Business continuity plans are important documents that set out how Local Health Districts can continue providing healthcare to people who need it when predictable events, such as floods, fire, storms and infrastructure failure (including cyber security incidents), occur. The NSW Cyber Security Policy includes a mandatory requirement for NSW Government entities to include cyber security in business continuity and disaster recovery planning.

Local Health Districts have limited mention of cyber security in their business continuity and disaster recovery plans. However, these disaster recovery and business continuity plans do not include detailed actions that consider bringing systems back online, workarounds for continuing to deliver patient care, or diversion to other services, privacy and data breaches and notification schemes.

In contrast with NSW Health's cyber security incident response planning, the audited Local Health Districts were able to demonstrate a degree of clinical input into business continuity planning. There is thus a clear opportunity for Local Health Districts to share cyber intelligence and approaches and for eHealth NSW to demonstrate leadership to improve the standard of these documents with respect to cyber security.

Local Health District disaster recovery plans complement business continuity plans. However, the audited Local Health Districts had incomplete or limited disaster recovery plans. Audited Local Health District disaster recovery plans did not clearly flow from or integrate with business continuity planning.

Appendix 1 – Response from entity

Response from NSW Health

NSW Health



Ref: H25/56220

Mr Bola Oyetunji
Auditor-General for New South Wales

NSW Health response to the performance audit on Cyber Security in Local Health Districts

Dear Mr Oyetunji

I refer to your letter of 28 May 2025, and I thank you for the opportunity to provide a response to your performance audit report *Cyber Security in Local Health Districts*.

The audit recommendations made for NSW Health are supported and will be implemented in an orderly manner. In accepting the recommendations, it is important to note the context of NSW Health's operating environment and the evolving cyber security threat landscape that all NSW Government Agencies face. Efforts are ongoing to improve state-wide policy directives, cross-agency working groups, and modern technical standards to navigate the devolved technical landscape while acknowledging shared risks and emerging threats.

NSW Health is committed to ensuring that our system is safe from cyber security threats and that the sensitive information we hold is safeguarded. A series of measures have been implemented in response to the findings of your report to strengthen our cyber security response and to enhance the overall capability of our system.

As part of these measures, I have established the NSW Health Cyber Security Taskforce to drive the implementation of reforms in this area, to coordinate capability uplift and to ensure the accountability of agencies within NSW Health. A dedicated Cyber Security Uplift Program has also been established to enhance cyber resilience across the health system, ensuring compliance with the NSW Cyber Security Policy and the Security of Critical Infrastructure (SOC) Act 2018. The program includes uplift across six key domains, being Essential Eight security controls, privileged access management, Crown Jewels (critical systems) protection, cyber security capabilities, risk and asset management and digital identity and zero trust architecture. Additional resourcing has been allocated to eHealth NSW to lead implementation of this state-wide reform, to respond to the audit recommendations and establish broader controls to enhance our approach to managing cyber security risks.

Further information regarding NSW Health's response to the audit report recommendations is included in the attached table. I would also like to acknowledge the support offered by the Audit Office of NSW during this audit and for the collaborative approach taken when working with representatives of NSW Health.

Yours sincerely

A handwritten signature in black ink, appearing to read "Susan Pearce".

Susan Pearce, AM
Secretary, NSW Health

Encl: NSW Health response to the Cyber Security in Local Health Districts Performance Audit recommendations

1 Reserve Road, St Leonards NSW 2065
Locked Mail Bag 2030, St Leonards NSW 1590

02 9391 9000
health.nsw.gov.au

1

NSW Health Response to Audit Recommendations

No.	Recommendation	Response
1	<p>By October 2025, the Ministry of Health should:</p> <p>Collate and validate information on compliance with NSW cyber security policy by each entity that reports to or via the Ministry of Health prior to annual attestation</p>	<p>Accepted</p> <p>eHealth NSW is the agency responsible for collating and validating information on compliance with the NSW Cyber Security Policy and will do so for the 2024/2025 annual attestation.</p>
2	<p>By December 2025, the Ministry of Health should:</p> <p>Finalise and communicate cyber security roles and responsibilities within the NSW Health system</p>	<p>Accepted</p> <p>eHealth NSW is working with NSW Health organisations, including the Ministry of Health, to update and communicate the Shared Responsibility Framework and ensure there is a shared understanding of key cyber security responsibilities and obligations.</p>
3	<p>By December 2025, eHealth NSW should:</p> <p>Work with the Ministry of Health to develop clear guidance for Local Health Districts on the obligation to manage the need to deliver clinical services while meeting critical cyber security requirements</p>	<p>Accepted</p> <p>eHealth NSW will work with the Ministry of Health to develop this guidance and deliver it through a dedicated cyber security education and awareness program of work.</p>
4.	<p>By December 2025, eHealth NSW should:</p> <p>Determine and apply sufficient resources to support the Privacy and Security Assessment Framework (PSAF) and Cyber Security Risk Assessments in Local Health Districts</p>	<p>Accepted</p> <p>eHealth NSW is undertaking a strategic review of current capabilities and resources to ensure that each LHD is equipped with the necessary expertise, tools, and support to meet PSAF requirements and conduct comprehensive cyber security risk assessments.</p> <p>This includes:</p> <ul style="list-style-type: none"> • Allocating dedicated personnel with privacy and cyber security expertise to support assessment activities. • Enhancing training and awareness programs to build local capacity and ensure consistent application of the PSAF. • Integrating assessment processes into broader clinical and digital governance frameworks to ensure alignment with operational and clinical system priorities. <p>These actions will help ensure that privacy and cyber security risks are proactively managed, particularly in relation to critical clinical systems and patient data, thereby strengthening the overall security posture of NSW Health.</p>

No.	Recommendation	Response
5.	<p>By December 2025, eHealth NSW should:</p> <p>Support Local Health Districts to improve cyber security capability by articulating a whole-of-health cyber security risk appetite statement:</p> <ol style="list-style-type: none"> a. providing direct assistance to localise centrally developed tools and frameworks b. ensuring all Local Health District crown jewel assets are monitored by the Health Security Operations Centre 	<p>Accepted</p> <p>eHealth NSW is working to develop a whole-of-health cyber security risk appetite statement, in collaboration with NSW Health LHDs.</p> <p>eHealth NSW will continue to assist Local Health Districts to:</p> <ul style="list-style-type: none"> • increase utilisation of the centrally provisioned cyber security tools and frameworks. • identify their local Crown Jewels and onboard them to the Health Security Operations Centre
6.	<p>By December 2025, Local Health Districts should:</p> <p>Design and implement a fit for purpose cyber security risk management framework incorporating:</p> <ol style="list-style-type: none"> a. an enterprise cyber security risk appetite statement, which aligns with the whole-of-health statement b. complete up-to-date cyber security and cyber security response plans, which are regularly tested and updated c. investment in establishing and maintaining Essential Eight cyber controls d. cyber security controls which identify and address the root causes of non-compliance and balance the need for clinical urgency with effective cyber security e. consideration of cyber security needs in the implementation of any new clinical systems 	<p>Accepted</p> <p>The Ministry of Health and eHealth NSW will collaborate with NSW Health LHDs to develop a structured program, including ongoing review and enhancement of controls, to progress these recommendations.</p>

Appendix 2 – About the audit

Audit objective and criteria

This audit assessed whether NSW Health is effectively safeguarding the clinical systems that are required to support healthcare delivery in Local Health Districts from cyber threats.

To address the audit objective, the following lines of inquiry and criteria were examined:

1. Do relevant NSW Health organisations effectively manage cyber security risks to clinical systems?
 - a) Relevant NSW Health organisations effectively consider the impact of a security incident on clinical systems and the subsequent effect on healthcare delivery when identifying critical data and information assets.
 - b) Cyber security planning considers a comprehensive range of threats to Local Health District assets when developing plans.
 - c) Local Health Districts' management of cyber security risks does not disrupt access to the clinical systems that are required to support healthcare delivery.
 - d) Local Health Districts demonstrate a strong culture of cyber security by ensuring that:
 - i) clinical staff are aware of and responsive to cyber security considerations
 - ii) clinical and non-clinical staff collaborate on cyber security issues.

2. Do relevant NSW Health organisations effectively respond to cyber attacks that affect selected clinical systems that are essential for service delivery?
 - a) Relevant NSW Health organisations effectively monitor the effectiveness of their cyber security controls.
 - b) Relevant NSW Health organisations effectively detect cyber security incidents in a reasonable timeframe.
 - c) Relevant NSW Health organisations effectively plan to respond to cyber incidents.
 - d) Relevant NSW Health organisations continually update and evaluate response plans as required to ensure they are fit-for-purpose.

Audit scope, focus and exclusions

This audit focused on assessing the performance of four selected Local Health Districts – the audited Local Health Districts – through the lens of one selected clinical service that is delivered at four hospital facilities within those Local Health Districts. The audited Local Health Districts include one metropolitan location, one outer-metropolitan location and two regional locations.

The audited clinical service was selected for its clinical importance. That is, any interruptions to the delivery of the selected clinical service could have detrimental impacts on patients if the issue is not resolved in 24 hours. Other factors were the accessibility of the selected service across NSW, the requirement to use clinical information and communication technology (ICT) systems to provide the service to patients, and services where Audit Office presence would not unduly elevate the risk of service disruption.

Each audited Local Health District was selected according to the following criteria: whether its hospital facilities deliver the selected clinical service; whether hospital facilities rely upon staff from other jurisdictions in arrangements such as Visiting Medical Officers; and participation in research or medical trials to address potential weaknesses or strengths in cyber security management.

The audited clinical service, hospital facilities and Local Health Districts remain confidential to ensure that risks, vulnerabilities and challenges can be identified and described within this audit report without placing impacted Local Health Districts at risk.

The audit did not question the merits of government policy objectives.

Audit approach

Our procedures included:

1. Interviewing
 - a) eHealth NSW staff:
 - i) relevant executive officers
 - ii) staff responsible for developing and providing cyber security-related guidance and advice to NSW Health entities.
 - b) Audited Local Health District staff:
 - i) relevant executive officers
 - ii) ICT staff
 - iii) clinical leaders and key clinical system users
 - iv) operational staff at hospital facilities, including clinical and non-clinical staff who interact with clinical systems.
2. Observing:
 - a) staff interaction with clinical systems.
3. Examining:
 - a) relevant eHealth NSW and audited Local Health District cyber security and risk documents.

The audit approach was complemented by quality assurance processes within the Audit Office to ensure compliance with professional standards.

Audit methodology

Our performance audit methodology is designed to satisfy Australian Auditing Standard ASAE 3500 Performance Engagements and other professional standards. The standards require the audit team to comply with relevant ethical requirements, and plan and perform the audit to obtain reasonable assurance and draw a conclusion on the audit objective. Our processes have also been designed to comply with requirements specified in the *Government Sector Audit Act 1983* and the *Local Government Act 1993*.

Acknowledgements

We gratefully acknowledge the cooperation and assistance provided by staff at eHealth NSW, the Ministry of Health and the audited Local Health Districts.

Audit cost

The estimated cost of the audit, including staff costs and overheads, is approximately \$600,000.

Appendix 3 – Performance auditing

What are performance audits?

Performance audits assess whether the activities of state or local government entities are being carried out effectively, economically, efficiently and in compliance with relevant laws.

The activities examined by a performance audit may include a government program, all or part of an audited entity, or more than one entity. They can also consider particular issues that affect the whole public sector and/or the whole local government sector. They cannot question the merits of government policy objectives.

The Auditor-General's mandate to undertake audits is set out in the *Government Sector Audit Act 1983* for state government entities, and in the *Local Government Act 1993* for local government entities. This mandate includes audit of non-government-sector entities where these entities have received money or other resources (whether directly or indirectly) from or on behalf of a government entity for a particular purpose (follow-the-dollar).

Why do we conduct performance audits?

Performance audits provide independent assurance to the NSW Parliament and the public.

Through their recommendations, performance audits seek to improve the value for money the community receives from government services.

How are performance audits selected?

When selecting and scoping topics, we aim to choose topics that reflect the interests of Parliament in holding the government to account. Performance audits are selected at the discretion of the Auditor-General based on our own research, suggestions from the public, and consultation with parliamentarians, agency heads and key government stakeholders. Our three-year performance audit program is published on our website and is reviewed annually to ensure it continues to address significant issues of interest to Parliament, aligns with government priorities, and reflects contemporary thinking on public sector management. Our program is sufficiently flexible to allow us to respond readily to any emerging issues.

What happens during the phases of a performance audit?

Performance audits have three key phases: planning, fieldwork and report writing.

During the planning phase, the audit team develops an understanding of the audit topic and responsible entities, and defines the objective and scope of the audit.

The planning phase also identifies the audit criteria. These are standards of performance against which the audited entity, program or activities are assessed. Criteria may be based on relevant legislation, internal policies and procedures, industry standards, best practice, government targets, benchmarks or published guidelines.

During the fieldwork phase, audit teams require access to books, records or any documentation deemed necessary in the conduct of the audit, including confidential information which is either Cabinet information within the meaning of the *Government Information (Public Access) Act 2009*, or information that could be subject to a claim of privilege by the state or a public official in a court of law. Confidential information will not be disclosed, unless authorised by the Auditor-General.

At the completion of fieldwork, the audit team meets with management representatives to discuss all significant matters arising from the audit. Following this, a draft performance audit report is prepared.

The audit team then meets with management representatives to check that facts presented in the draft report are accurate, and to seek input in developing practical recommendations on areas of improvement.

A final report is then provided to the accountable authority of the audited entity(ies), who is invited to formally respond to the report. If the audit includes a follow-the-dollar component, the final report will also be provided to the governing body of the relevant entity. The report presented to the NSW Parliament includes any response from the accountable authority of the audited entity. The relevant Minister and the Treasurer are also provided with a copy of the final report for state government entities. For local government entities, the Secretary of the Department of Planning, Housing and Infrastructure, the Minister for Local Government and other responsible Ministers will also be provided with a copy of the report. In performance audits that involve multiple entities, there may be responses from more than one audited entity or from a nominated coordinating entity.

Who checks to see if recommendations have been implemented?

After the report is presented to the NSW Parliament, it is usual for the entity's Audit and Risk Committee/Audit Risk and Improvement Committee to monitor progress in implementing recommendations.

In addition, it is the practice of NSW Parliament's Public Accounts Committee to conduct reviews or hold inquiries into matters raised in performance audit reports. The reviews and inquiries are usually held 12 months after the report is received by the NSW Parliament. These reports are available on the NSW Parliament website.

Who audits the auditors?

Our performance audits are subject to internal and external quality reviews against relevant Australian standards.

The Public Accounts Committee appoints an independent reviewer to report on compliance with auditing practices and standards every four years. The reviewer's report is presented to the NSW Parliament and is available on its website.

Periodic peer reviews by other audit offices test our activities against relevant standards and better practice.

Each audit is subject to internal review prior to its release.

Who pays for performance audits?

No fee is charged to entities for performance audits. Our performance audit services are funded by the NSW Parliament.

Further information and copies of reports

For further information, including copies of performance audit reports and a list of audits currently in progress, please see our website www.audit.nsw.gov.au or contact us on 9275 7100.

OUR VISION

Our insights inform and challenge government to improve outcomes for citizens.

OUR PURPOSE

To help Parliament hold government accountable for its use of public resources.

OUR VALUES

Pride in purpose
Curious and open-minded
Valuing people
Contagious integrity
Courage (even when it's uncomfortable)



Audit Office of New South Wales

Level 19, Darling Park Tower 2
201 Sussex Street
Sydney NSW 2000 Australia

t +61 2 9275 7100

mail@audit.nsw.gov.au

Office hours: 8.30 am–5.00 pm

audit.nsw.gov.au