
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 (SOCl) 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

25/6/25

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>