
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.