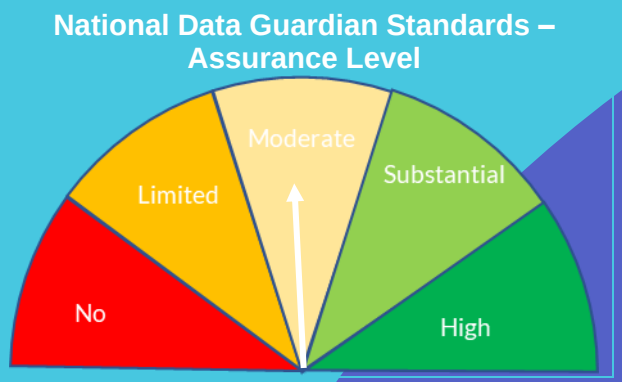
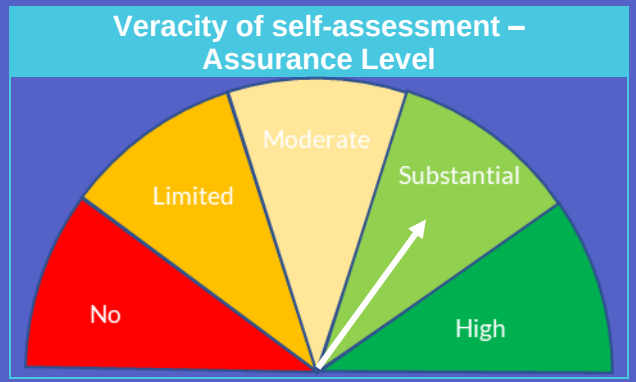
Data Security and Protection Toolkit Assignment Report 2023/24 (Final)

Warrington and Halton NHS Foundation Trust

106WHFT_2324_902





Contents

Executive Summary

Assessment and Assurance

Appendix A: Terms of Reference

Appendix B: Assurance Definitions and Risk Classifications

Appendix C: Report Distribution

MIAA would like to thank all staff for their co-operation and assistance in completing this review.

This report has been prepared as commissioned by the organisation, and is for your sole use. If you have any queries regarding this review please contact the Engagement Manager. To discuss any other issues then please contact the Director.

1 Executive Summary

Key Findings/Conclusion

This review of Warrington and Halton NHS Foundation Trust Data Security and Protection Toolkit (DSPT) assessment has been completed in line with the DSPT Strengthening Assurance Guide and published methodology for independent assessment for the in-scope assertions and key elements of the DSP Toolkit environment.

The review comprised of an assessment of the overall risk associated with the organisation's data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved and an assessment as to the veracity of the organisation's self-assessment / DSP Toolkit submission and the assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

The Trust has demonstrated a clear organisational structure with associated key roles in place that included job descriptions clearly relating the specific job role. The Trust had 2 separate contracts in place (standard contract and band 9 or greater) – both contracts referenced data protection and confidentiality. The Trust had a training needs analysis in place which contained a wide range of staff including those in key roles – this had been agreed by the information governance and records sub-committee. NHS mail is in place across the organisation.

However, a number of areas were identified which required improvement, including third parties having the appropriate accreditations such as CE+ / ISO 27001. MFA arrangements were not in place for users remote accessing onto the network.

A number of low risks identified also included; The information asset register which was currently a work in progress aligning the headings to match NHS England's standards.

Assertion number	RAG Rating
1.1	
2.2	
3.1	
3.2	
4.4	
5.1	
6.2	
7.1	
8.4	
9.2	
9.5	
9.6	
10.2	

Areas of Good Practice

- The governance structure was found to be in place and operating effectively (1.1.5);
- Employment contracts included relevant data protection and confidentiality clauses (2.2.1);
- Training needs analysis has been agreed at board level and contained relevant staff roles (3.1.1);
- Privileged users that have access to an Admin account do not have any access to emails on that account and have limited internet access. A sample test was conducted to show that users use their normal account for day to day tasks (4.4.2);
- Regular root cause analysis was undertaken to identify key themes of Information Governance and Cyber security incidents (5.1.1);
- A sample test of 10 endpoints and 10 servers revealed that they all have antivirus enabled on the devices and they all had the latest patch applied (6.2.4, 8.4.2);
- NHS mail was in place across the organisation (6.2.8 / 6.2.9);
- Business continuity exercises such as Supply Chain Compromise and Cyber Escalation Incident Response Scenarios had been conducted, incident response plans for data loss, denial of service, ransomware, malware and phishing were in place (7.1.1);
- There were multiple examples of threat intelligence sources in place across the organisation as well as a documented patching deployment strategy (8.4.1);
- Change management processes were in place and they all go through the change management share portal. The Trust also had a IT change enablement policy outlining the process (9.5.3, 9.6.4);
- Microsoft defender firewalls were enabled on all devices, a sample test of 10 users shown that it was active on the devices.

Areas of vulnerability and / or opportunities for improvement	
Medium	• Ensure that third parties have the substantial accreditations and Roles and responsibilities are documented. • Ensure that MFA arrangements are in place for users remote accessing onto the network.
Low	• Continue to populate the information asset register so that it aligns with NHS England's headings and data, as planned. • Document and formalise the build process for blank workstations, including the implementation of antivirus on the device. • Out of date documentation such as Business Continuity Plans should be ratified prior to submission. • Implement Cynerio when possible, to gain a wider understanding of the IoT devices across the organisation. • Continue to remove out of support Operating systems such as Windows 2008 and Windows 2012, as planned. • The Trust should create and formalise documentation that shows automatic logging taking place along with a proactive log review schedule. • Evidence the logging policies in technical controls i.e configuration screens to demonstrate that applications are set as per policy. • Ensure that the penetration testing exercise is conducted, with an action plan for its findings.

Assessment and Assurance

2. 1 Assessment of self-assessment

In our view, the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment and, as such, the assurance level in respect of the veracity of the self-assessment is:

Substantial

2.2 Assessment against National Data Guardian Standards

Across the National Data Guardian Standards our assurance ratings, based upon criteria at Appendix B are:

National Data Guardian Standard level	Overall assurance rating at the National Data Guardian level
1. Personal Confidential Data	● Substantial
2. Staff Responsibilities	● Substantial
3. Training	● Substantial
4. Managing Data Access	● Substantial
5. Process Reviews	● Substantial

National Data Guardian Standard level	Overall assurance rating at the National Data Guardian level
6. Responding to Incidents	Substantial
7. Continuity Planning	Substantial
8. Unsupported Systems	Substantial
9. IT Protection	Moderate
10. Accountable Suppliers	Moderate

The rating is based on a mean risk rating score at the National Data Guardian (NDG) standard level. Scores have been calculated using the guidance from the independent assessment Guidance document.

As a result of the above, our overall assurance level across all 10 NDG Standards is rated as:

Moderate

Appendix A: Terms of Reference

Our work aimed to assess and provide assurance based upon the validity of the organisation's intended final submission, and consider not only if the submission is reasonable based on the evidence submitted, but also provide assurance based on the extent to which information risk has been managed in this context.

Our scope was based on that recommended as part of the Data Security and Protection (DSP) Toolkit Strengthening Assurance Guide published in 2023 by NHS England. As such our assessment involved the following steps:

- Obtain access to your organisation's DSP Toolkit self-assessment.
- Discuss the mandatory assertions that will be assessed with your organisation and define the evidence texts that will be examined during the assessment.
- Request and review the documentation provided in relation to evidence texts that are in scope of this assessment prior to the audit (if applicable).
- Interviewing the relevant stakeholders as directed by the organisation lead, who are responsible for each of the assertion evidence texts/self-assessment responses or people, processes and technology.
- Review the operation of key technical controls on-site using the DSP Toolkit Independent Assessment Framework as well as exercising professional judgement and knowledge of the organisation being assessed.

Selected Assertions

As based on the recommended scoping from NHS digital the selected thirteen assertions are as follows:

Area	Description
1.1	The organisation has a framework in place to support Lawfulness, Fairness and Transparency
2.2	Staff contracts set out responsibilities for data security
3.1	Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness

3.2	Your organisation engages proactively and widely to improve data security, and has an open and just culture for data security incidents
4.4	You closely manage privileged user access to networks and information systems supporting the essential service
5.1	Process reviews are held at least once per year where data security is put at risk and following DS incidents
6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway
7.1	Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services
8.4	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service
9.2	A penetration test has been scoped and undertaken
9.5	You securely configure the network and information systems that support the delivery of essential services
9.6	The organisation is protected by a well-managed firewall
10.2	Basic due diligence has been undertaken against each supplier that handles personal information

The scope of this review included only the mandatory elements of the above selected assertions.

Appendix B: Assurance Definitions and Risk Classifications

Overall NDG Standard	Rating Thresholds	Rating Thresholds when 2 or more assertions are in	Assurance Rating Classification	when only 1 assertion per NDG Standard is in scope	scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions)

Substantial	1 or less	1 or less
Moderate	Greater than 1, less than 10	Greater than 1, less than 4
Limited	Greater than/equal to 10, less than 40	Greater than/equal to 4, less than 5.9
Unsatisfactory	40 and above	5.9 and above

Unsatisfactory	1 or more Standards is rated as 'Unsatisfactory'
Limited	No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited'
Moderate	There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'.
Substantial	All of the standards are rated as 'Substantial'

Overall risk rating across all in-scope standards

Level of deviation from the DSP Toolkit submission and assessment findings

Confidence level

Assurance level

High – the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment

For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.

Medium - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment

For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two.

Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment

Appendix C: Report Distribution

Name	Title
Jane Hurst	Director of Finance
Paul Fitzsimmons	Medical Director (Caldicott Guardian)
Tom Poulter	Chief Information Officer
Sue Caisley	Deputy Chief Information Officer
Mark Ashton	Information Governance and Corporate Records Manager and Data Protection Officer (DPO)
Stephen Deacon	Head of Digital Compliance

Conor Finegan
Technology Risk Auditor
Tel: 07825 100 276
Email: Conor.Finegan@miaa.nhs.uk

Paula Fagan
Head of Technology Risk
Tel: 07825 592 866
Email: Paula.Fagan@miaa.nhs.uk

Lesley Silcock
Principal Digital Risk Consultant
Tel: 07557 168 506
Email: Lesley.Silcock@miaa.nhs.uk

Limitations

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards and conforms with the International Standards for the Professional Practice of Internal Auditing.