Data Security and Protection Toolkit Assessment Summary Report 2022/23 (Final)

The Walton Centre NHS Foundation Trust

Report Ref: 108WCFT_2223_901

Date of Issue: 12th June` 2023

Contents

Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

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.

Future periods

The assessment of controls relating to the process is that at May 2023. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards.

Key Dates

Report Stage	Date
Discussion Document Issued	30/05/2023
Discussion Meeting	30/05/2023
Final Draft Report Issued	05/06/2023
Client Approval Received	09/06/2023
Final Report Issued	12/06/2023

Report Distribution

Name	Title
Mike Burns	Chief Finance Officer (SIRO)
Sacha Niven	Deputy Medical Director (Caldicott Guardian)
Justin Griffiths	Chief Digital Information Officer
Lorraine Robinson	Information Governance Manager

Audit Team

Name	Contact Details	
Michael McCarthy	Michael.McCarthy@miaa.nhs.uk	07552 258 920
Conor Finegan	Conor.Finegan@miaa.nhs.uk	07825 100 276
Paula Fagan	Paula.Fagan@miaa.nhs.uk	07825 592 866

Acknowledgement and Further Information

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 Senior Technology Risk Assurance Manager. To discuss any other issues then please contact the Head of Technology Risk Assurance. MIAA would be grateful if you could complete a short survey using the link below to provide us with valuable feedback to support us in continuing to provide the best service to you.
https://www.surveymonkey.com/r/MIAA_Client_Feedback_Survey

1 Introduction, Background and Objective

In 2018 the Information Governance toolkit (IGT) was withdrawn and replaced with the new Data Security and Protection Toolkit (DSPT). It was developed by NHS Digital in response to The National Data Guardian's Review of Data Security, Consent and Opt-Outs published in July 2016 and the subsequent Government response, Your Data: Better Security, Better Choice, Better Care, published in July 2017.

The DSPT is a tool which allows organisations to measure their compliance against legislation and central guidance, and helps identify areas of full, partial or non-compliance.

In July 2021, NHS Digital published a methodology for independent assessment and internal audit providers to implement when performing DSPT audits for 2022/23 which included a set scope for the review.

The published assessment methodology requires assessors/auditors to form a view on the in-scope assertions and key elements of your DSP Toolkit environment including:

- 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;
- 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 guidance also provides a reporting and scoring standard.

Whilst this guidance has formed the basis of our approach, we have had to apply flexibility and pragmatism to the approach given the impacts and challenges for organisations during the ongoing coronavirus pandemic. As such, review and assessment in some instances has been based on evidence as provided rather than that independently obtained.

2 Scope

In accordance with the guidance mandated by NHS Digital, the selected thirteen DSPT assertions assessed during this review were:

Area	Description
1.3	Accountability and Governance in place for data protection and data security
2.1	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards
3.4	Leaders and Board members receive suitable data protection and security training

Area	Description
4.1	The organisation maintains a current record of staff and their roles
4.2	The organisation assures good management and maintenance of identity and access control for its networks and information systems
4.5	You ensure your passwords are suitable for the information you are protecting
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents
6.3	Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses
7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions
8.3	Supported systems are kept up-to-date with the latest security patches
9.3	Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities
10.1	The organisation can name its suppliers, the products and services they deliver and the contract durations

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

3 Executive Summary

The Walton Centre NHS Foundation Trust is a specialist hospital delivering neurology, neurosurgery, spinal and pain management services.

The Trust have demonstrated a framework was in place in relation to data security and protection with commitment and support by senior management. There was a defined organisational structure with associated committees and supporting policies and procedures were in place.

The Trust has demonstrated its plans for the completion of its toolkit submission in time for the June 2023 submission.

3.1 Areas of good practice

During our review we noted the following areas of good practice:

- There was a range of IG policies and procedures in place which where all within their review period (1.3.1).
- A clear governance structure for IG and IT had been documented. The governance structure was found to be in place and operating effectively (1.3.4).
- It was identified that data security and protection risks were being managed in line with the risk management policy and the Trust had identified it's top 3 risks in this area (1.3.5 & 1.3.6).
- The Trust had a Data Privacy Impact Assessment (DPIA) process in place with oversight of the process delegated to the Information Governance Security Forum (IGSF) (1.3.8).
- Responsibility for data protection and security had been delegated by the Board to the Business Performance Committee and ultimately the IGSF (1.3.9).
- At the time of the review, all members of the Trust Board had completed their mandatory data security awareness training in line with the approved Training Needs Analysis (3.4.2).
- Testing undertaken on a sample of leavers identified that each had their access removed in line with the Personnel Security and Access Controls standard. None of the sampled leavers had accessed their accounts subsequent to their termination date (4.2.1 & 4.2.4).
- The Trust had a Monitoring and Auditing Standard which governed the review and collection of activity logs. We were provided evidence that user activity logs were retained for at least 6 months (4.2.3).
- There was a robust incident management and root cause analysis (RCA) process in place at the Trust. Since July 2022, there had been one incident that required an RCA to be undertaken. Review of the associated documentation identified that the RCA had been completed in line with the Incident Reporting Policy (5.1.1).
- Furthermore, we were informed that there were no data security incidents that had resulted from a known vulnerability (6.3.1).
- There was an IT Business and Disaster Recovery Policy in place and there was evidence the Trust had in-house resource that could be deployed in the event of a data security incident (7.3.1).
- The Trust could demonstrate that backups of critical systems were tested on a monthly basis (7.3.5).

- Testing undertaken on a sample of endpoints and servers identified that each had been patched in line with the Cyber Security Standard. The Trust had the ability to automatically deploy patches to endpoints which was documented within the Cyber Security Standard (8.3.1 & 8.3.2).
- There was evidence that the Trust was actively using Advanced Threat Protection (ATP) and Microsoft Defender for Endpoint (MDE) as a key part of the cyber security monitoring tooling (8.3.6).
- The Trust was registered for and was actively using the NCSC's suite of services including the early warning service and the Webcheck service (8.3.8 & 9.3.7).
- There was a technical solution in place to block connections to malicious websites which was provided by the Trend system (9.3.3).
- The Trust provided evidence that it was proactively reviewing administrative users with access to the domain controllers. Furthermore, the Trust was reviewing activity taken within the domain controllers including changes to the authoritative DNS entries (9.3.4).

3.2 Areas of vulnerability and/or where improvement is required

Our detailed findings and recommendations are described in more detail in a spreadsheet that has been provided under separate cover in order that vulnerabilities are not described in detail within this document. The spreadsheet should be treated as confidential as disclosure, without significant redaction, may result in any vulnerabilities becoming more widely known and exploited.

The key areas identified, however, can be summarised thus:

- A significant amount of the Trust's server estate was operating on unsupported operating systems such as Windows Server 2000 and Server 2008 R2. It was noted that there was a plan in place to remove these server operating systems from the environment (8.3.7).
- At the time of the review, the Trust was not assured that all connected medical devices across the estate had been identified. Furthermore, it was not clear who was responsible for the maintenance and update of each class of medical device. We were informed that this was a work in progress across the Trust (9.3.8 & 9.3.9).
- During the review, the Trust had not approved the IG Annual Report which included details of the audit and spot check activity undertaken by the Information Governance Team (1.3.2).
- Testing undertaken on a sample of 10 new starters identified that 2 had not completed their mandatory data security awareness training in line with the Induction and Mandatory Training Policy. It was unclear if the Trust had attempted to remediate the non-compliance with the specific new starters (2.1.1).
- The TNA had not been reviewed and approved in line with its scheduled review date of 31/3/23 (3.4.1).

- The Trust would benefit from documenting its plan for the introduction of Privileged Access Management (PAM) and Multi-factor Authentication (MFA) in a strategy or similar (4.1.1 & 4.5.3).
- As planned, the Trust should continue to implement the LogOnBox solution to provide a password deny list functionality and increase the security of login credentials across the estate (4.5.2).
- The Trust should develop a cyber security strategy with consideration of the proposed Cheshire and Merseyside Integrated Care System (ICS) Cyber Security Strategy. The Trust should consider documenting any gaps in the cyber security monitoring processes once the strategy is in place (6.3.3).
- It was identified that the Trust could make improvements to its fraud risk assessments process. For example, include documenting which systems have been assessed to be attractive to cyber criminals and the controls in place to mitigate the risk posed (6.3.4).
- As planned, the Trust should complete, document and report the completion of a disaster recovery and business continuity exercise ahead of submission (7.2.1 & 7.2.2).
- Although the Trust had Recovery Time and Recovery Point Objectives (RTO/RPO) identified for each system, it was confirmed that these had not been agreed by the Information Asset Owners (IAOs). Therefore, there was no assurance that RTO and RPO for each system was suitable for the criticality of the system (7.3.4).
- The Trust should review its Cyber Security Standard to include the specific process for the SIRO risk acceptance of critical security updates that cannot be remediated within 14 days or at all. It was noted that 2 of the 10 high risk NHS Cyber Alerts tested had not been remediated within 14 days and there was no evidence of explicit risk acceptance by the SIRO (8.3.3, 8.3.4 & 8.3.5).
- As planned, the Trust should ensure its software development staff have been trained in secure design principles (9.3.1).
- Prior to submission, the Trust should ensure that the contracts register is fully completed. It was noted that there was a development plan in place for the supplier management process at the Trust (10.1.1).

4 Assessment and Assurance

4.1 Assessment of self-assessment

In our view, the self-assessment against the Toolkit 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

4.2 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
6. Responding to Incidents	Substantial
7. Continuity Planning	Substantial
8. Unsupported Systems	Moderate
9. IT Protection	Moderate
10. Accountable Suppliers	Substantial

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 2022 by NHS Digital. 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
1.3	Accountability and Governance in place for data protection and data security
2.1	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards
3.4	Leaders and Board members receive suitable data protection and security training
4.1	The organisation maintains a current record of staff and their roles

Area	Description
4.2	The organisation assures good management and maintenance of identity and access control for its networks and information systems
4.5	You ensure your passwords are suitable for the information you are protecting
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents
6.3	Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses
7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions
8.3	Supported systems are kept up-to-date with the latest security patches
9.3	Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities
10.1	The organisation can name its suppliers, the products and services they deliver and the contract durations

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 Assurance Rating Classification	Rating Thresholds when only 1 assertion per NDG Standard is in scope	Rating Thresholds when 2 or more assertions are in 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

Overall risk rating across all in-scope standards

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'

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'.	Low	Limited
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.	Medium	Moderate
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment	High	Substantial