Data Security and Protection Toolkit Assessment Summary Report 2021/22 (Final)

The Walton Centre NHS Foundation Trust

Report Ref: 105WCFT_2122_902

Date of Issue: 16th August 2022

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 in May/June 2022. 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	30th June 2022
Discussion Meeting	30th June 2022
Final Draft Report Issued	30th June 2022
Client Approval Received	
Final Report Issued	16th August 2022

Report Distribution

Name	Title
Mike Burns	Chief Finance Officer and IT (SIRO)
Sacha Niven	Deputy Medical Director (Caldicott Guardian)
Justin Griffiths	Head of IM&T
Lorraine Blyth	Information Governance Manager

Audit Team

Name	Contact Details	Mobile
Peter Mulford	Peter.Mulford@miaa.nhs.uk	07880 472 641
Gemma Owens	Gemma.Owens@miaa.nhs.uk	07717 720 389
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 2021/22 (https://www.dsptoolkit.nhs.uk/News/83) 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.

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
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 with plans to update/reapprove those that had passed their review date.

The Trust has demonstrated its plans for the completion of its toolkit submission in time for the June 2022 submission.

3.1 Areas of good practice

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

- Key policies were in place, in date and evidence of ratification provided. (1.3.1);
- Evidence on the completion of ward confidentiality audits being completed, however the Trust should ensure action plans are formalised and monitored for implementation. (1.3.2 & 2.2.1 & 4.2.1);
- The Trust identified their top 3 data security and protection risks and their sign off by the SIRO. (1.3.6);
- Defined processes in place for data protection by design and default principles with reporting to key committee within governance structure. (1.3.8);
- Data security evident on Board agenda with leadership from SIRO and annual reporting providing updates on aspects such as the information governance framework, risk analysis and cyber security arrangements. (1.3.9)
- New starter training process defined with records demonstrating attendance. (2.1.1 & 4.1.1);
- Contractual arrangements are in place for permanent staff, bank, volunteers, and temporary staff. (2.1.2 & 4.1.1);
- Process in place and operating with regards to maintaining staff and their roles. (4.1.1);
- Access control to the Trust's assets / systems was found to be well managed. (4.1.2, 4.2.1, 4.2.4);
- Data security and protection incidents were being reported and investigated with root cause analysis and lessons learned demonstrated. Responses to high severity cyber alerts were within 48 hours for testing sample. (5.1.1, 6.3.1 & 6.3.2);

- The Trust demonstrated a proportionate approach to monitoring solutions were in place to detect cyber events on systems and services. (6.3.3, 9.3.8);
- The ICT Disaster Recovery Plan detailed the location of emergency contacts identified. (7.3.2);
- The Trust confirmed how it was managing backups. Backup arrangements were being strengthened with a business plan for new solution and immutable backups . (7.3.4, 7.3.5, 7.3.6);
- Approach to applying security updates (patching) to end users, including management of NHS Digital alerts (CareCERTs) was demonstrated. (8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5);
- The Trust were able to demonstrate how they record IP ranges in use across the organisation. (9.3.5);
- A centralised asset management solution was in place, this contained key data in relation to suppliers and identified the processing of personal data and services provided. (10.1.1).

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:

- The Trust should ensure that the DPIA register is scheduled for review on at least a bi-annual basis. (1.3.8);
- Ensure all outstanding training for Board members, including specialist training, has completed their training, as planned. (1.3.9, 3.4.1 & 3.4.2);
- The Trust should review contract wording to ensure that they reflect the most current legislation and guidance with regards to data security requirements. (2.1.2 & 4.1.1);
- The Trust should look to include the minimum standard for log retention within corporate policy. It is recommended that logs are retained for a minimum of six months to enable their use for the detection of potential malicious activity. (4.2.3)
- Password policies, including those for privileged system accounts were found to be in place. The Trust should however ensure there is sufficient process in place to address password blacklisting as well as extend MFA where possible. (4.5.1, 4.5.2, 4.5.3, 4.5.4);
- Formalise the process for the assessment of new digital systems transactional monitoring. 6.3.4 & 10.1.1);

- The Trust should continue with its plans for a test of its data security incident response and management plan as well as a penetration test before DSPT submission with results of the tests reported to the SIRO. (7.2.1, 7.2.2, 9.3.2);
- The Trust needs to ensure there is adequate provision for forensic support (where appropriate) either in house or external. (7.3.1);
- The Trust should ensure there are adequate RTO/RPOs defined for key systems. (7.3.4);
- The Trust should ensure there is a robust process in place detailing how servers will receive timely updates. (8.3.1);
- The Trust needs to strengthen their ability to demonstrate there is SIRO sign off on the application of updates. (8.3.5);
- The Trust should ensure the contracts register is fully completed with key information including the handling of personal information. (10.1.1);

4 Assessment and Assurance

4.1 Assessment of self-assessment

In our view, the self-assessment does not differ materially from our independent assessment and, as such, the assurance level in respect of the veracity of the self-assessment is:

Substantial Assurance

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	Substantial
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 Assurance

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 2021 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
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 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