Royal Devon University Healthcare NHS Foundation Trust

DSP Toolkit - External Auditor Assessment

Reference Number: RDF2225-24
Date of Response: 13/02/24

Further to your Freedom of Information Act request, please find the Trust's response(s) below:

I would be grateful to receive a copy of your DSP Toolkit External Auditor Assessment for last year (22/23).
Answer: We confirm we hold the information requested but are withholding some of this under Section 31(1), Section 43(2) and Section 40(2) of the Freedom of Information Act 2000.
Please see file attached: *RDUHFT0124A - DSPT Assessment Part Two Report – Redacted.pdf*

Section 31(1)
Section 31(1) of the FOIA allows a public authority to withhold / exempt information if its disclosure would or would be likely to prejudice the prevention or detection of crime and the exercise of its functions, including securing the health, safety and welfare of persons.

The public interest test
Section 31 exemptions are subject to the public interest test. There are several factors that must be considered and weighed up. The factors we have considered are set out below.

Factors in favour of disclosure:

- It would promote openness and transparency of the Trust's data security.

- It would reassure people about how secure and effective the Trust's IT infrastructure and systems are.

Factors against disclosure:

- Disclosure of this information about how effective the Trust's data security, IT infrastructure and systems are would likely give cyber criminals insight into the strengths of the Trust's IT infrastructure and systems and any potential weaknesses that may exist. This would increase the chances of cyberattacks. One of the reasons that cyber security measures are in place is to protect the integrity of personal and sensitive personal information, so increasing the chances of an attack would have potentially serious repercussions.

- If the Trust discloses the information requested, then this could show criminals and threat actors its infrastructure and systems are particularly vulnerable and encourage attacks.

- If the Trust discloses the information requested, this could either show it has weaknesses in its data security and IT systems which will encourage an attack, or it could show it has robust procedures which could encourage an attack to

try out criminals' new techniques or could encourage criminals to target other Trust's which would increase crime elsewhere.

- There is public interest in protecting patient and staff personal data and preventing any threat to the integrity of Trust's data and IT infrastructure systems.

- There is public interest in complying with the Trust's legal obligations to keep personal data secure and to take appropriate measures which includes maintaining and improving data security and protection.

- The costs to the Trust associated with recovery from a cyber-attack including updating/changing systems, new software, revenue and regulatory fines.

- Public interest in avoiding significant disruption to health service provision by the Trust.

- Cyber-attacks which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks and since it holds substantial amounts of sensitive, personal, and confidential information, maintaining the security of this information is essential.

- In this context, the Trust considers that providing the requested information would also provide information about the Trust's information systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Releasing the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

- As an Operator of Essential Services the Trust must comply with The Network and Information Systems Regulations 2018. (https://www.legislation.gov.uk/uksi/2018/506/schedule/2/paragraph/8)

  By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in Section 10 (https://www.legislation.gov.uk/uksi/2018/506/regulation/10) of the Network and Information Systems Regulations 2018.

The prejudice in complying with Section 31 of FOIA is real and significant as it would allow valuable insight into the perceived strengths and weaknesses of the Trust's IT infrastructure and information systems. On balance, the Trust concludes that the balance of public interest lies in upholding the exemption and exempting by redaction certain sections of the DSP Toolkit assessment.

Section 42(2)
Some of the information requested is considered commercially sensitive, and its release would or would be likely to prejudice the commercial interests of the Trust.

In applying the exemption under Section 43(2) the Freedom of Information Act the Trust has balanced the public interest in withholding the information against the public interest in disclosure. The Trust has considered all the relevant factors in the public interest test and concluded that the benefit to the public in applying the exemption outweighs the public interest in disclosing the requested information because of the prejudices and losses that would potentially affect the Trust and its patients. As such this information is being withheld under Section 43 (2) and only certain sections of the DSP Toolkit assessment are being disclosed.

Section 40(2)
Please note staff names have been withheld/ redacted from the assessment because these are exempted under Section 40 (2) of the Freedom of Information Act. The Trust recognises that this is personal information, and its disclosure would be in breach of the Data Protection Act principles.

The outcomes of the Trust's Data Security and Protection Toolkit self-assessments are published by NHS England. Please see link:
https://www.dsptoolkit.nhs.uk/OrganisationSearch/RH8

ASW Assurance
Sharing excellence in governance

NHS

Royal Devon University Hospitals NHS Foundation Trust
Final Data Security and Protection Toolkit Assessment Summary - Part Two Report 2022/2023

Report Reference: RDUHFT01/24A
June 2023

Distribution List (for action):

- [redacted]
- [redacted]

Additional Copies (final report, for information):

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Executive Summary

AUDIT BACKGROUND, SCOPE AND OBJECTIVES

Background

The Data Security and Protection Toolkit (DSPT) allows organisations to measure their compliance against law and central guidance, and helps identify areas of full, partial or non-compliance. There is a contractual obligation for providers to complete the DSPT and they are subject to audit against it.

In September 2021, NHS Digital published an assessment methodology for independent assessment and internal audit providers to implement when performing such audits, which included a set scope for the review. As such, this work was carried out in accordance with those requirements.

The published assessment methodology requires Internal Audit to form a view on the in-scope assertions and key elements of the DSPT 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 / DSPT 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.

For the first time this year, NHS England require the auditors to upload the audit report to the DSPT.

Objectives and Scope of the Audit

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

The scope of this review was based on that recommended as part of the DSPT Independent Assessment Guides published in 2022 by NHS Digital. In accordance with the guidance mandated by NHS Digital, the thirteen DSPT assertions assessed during this work are documented overleaf.

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 (NDG) 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 Network 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.

OVERALL CONCLUSION

It should be noted when reading the conclusions and findings of this report, that at the time of our review, the Trust had not fully completed the integration of the Digital Services teams which include the Information Governance and Cyber Security activities of Eastern and Northern Services. [redacted] As such, to conduct our review, we had to assess both individual assessments separately and review the evidence provided to compose our findings and conclusions.

We assessed the Trust's overall risk rating as per the definitions set by National Data Guardian (NDG) Standards (NHS Digital - see Appendix A) for the assertions reviewed as [redacted] based upon the evidence provided for review.

Although both Northern and Eastern Services have an overall assessment of [redacted] as is demonstrated in the assessment against the NDG standards overleaf, there is a disparity between our two reviews due to the level of evidence provided, [redacted]

We note that in this, our Part Two review, the disparity is less than that identified in the Part One review with the evidence base for Northern Services has improved against the NDG standards for both Process Reviews and Accountable Suppliers improving from [redacted] Our confidence in the veracity of the organisation's self-assessment is [redacted]

We have highlighted areas where the evidence base needs to be improved. These have been summarised in the vulnerabilities section of this report.

Assessment and Assurance

Assessment of 'self-assessment' At the conclusion of the review the organisation had not fully completed the in-scope standards within the toolkit and had yet to submit its self-assessment against the toolkit which is due at the end of June, 2023.

Assessment against NDG Standards

Across the NDG Standards our assurance ratings, based upon criteria at Appendix A and as at the time of our review were:

National Data Guardian (NDG) Standard	Overall Risk Rating at the NDG Standard Level		National Data Guardian (NDG) Standard	Overall Risk Rating at the NDG Standard Level	
	Eastern Services	Northern Services		Eastern Services	Northern Services
1. Personal Confidential Data	[redacted]		6. Responding to Incidents	[redacted]	
2. Staff Responsibilities			7. Continuity Planning		
3. Training			8. Unsupported Systems		
4. Managing Data Access			9. IT Protection		
5. Process Reviews			10. Accountable Suppliers		

The risk rating is based on a mean risk score at the National Data Guardian 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 National Data Guardian Standards is rated as **Moderate** for both Eastern and Northern Services.

Our overall conclusion is supported by the following good practice and vulnerability conclusions set out below:

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Appendix A: Assurance Definitions and Risk Classifications

Overall NDG Standard Risk 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
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**
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**
Low - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment.	**High**

ASW Assurance – About Us

ASW Assurance is the largest provider of internal audit, counter fraud and consultancy services in the South West. We maintain a local presence and close engagement within each health community, with audit teams based in Bristol, Exeter, North Devon, Plymouth, Torquay and Cornwall, linked by shared networks and systems. More information about us, including the services we offer, our client base, our office locations and key people can be found on our website at www.aswassurance.co.uk.

ASW Assurance is a member of TIAN; a group of NHS internal audit and counter fraud providers from across England and Wales. Its purpose is to facilitate collaboration, share best practice information, knowledge and resources in order to support the success and quality of our client's services.

All audit and assurance assignments are conducted in conformance with the International Standards for the Professional Practice of Internal Auditing.

Confidentiality

This report is issued under strict confidentiality and, whilst it is accepted that issues raised may need to be discussed with officers not shown on the distribution list, the report itself must not be copied/circulated/disclosed to anyone outside of the organisation without prior approval from the Director of Audit and Assurance Services.

Inherent Limitations of the Audit

There are inherent limitations as to what can be achieved by systems of internal control and consequently limitations to the conclusions that can be drawn from this review. These limitations include the possibility of faulty judgment in decision-making, of breakdowns because of human error, of control activities being circumvented by the collusion of two or more people and of management overriding controls. Also, there is no certainty that controls will continue to operate effectively in future periods or that the controls will mitigate all significant risks which may arise in future. Accordingly, unless specifically stated, we express no opinion about the adequacy of the systems of internal control to mitigate unidentified future risk.

Rating of Audit Recommendations

The recommendations in this report are rated according to NHS Digitals risk-scoring matrix.

ASW Assurance

Sharing excellence in governance

Get in touch

www.aswassurance.co.uk