

# **Data Security and Protection Toolkit Independent Assessment**

**Bradford Teaching Hospitals  
NHS Foundation Trust  
BH/xx/2023**



## Contents

<b>1. Executive summary</b>	<b>1</b>
<b>2. Detailed Report</b>	<b>2</b>
Appendices	
Appendix A: Risk and Confidence Evaluation	<b>7</b>
Appendix B: The Ten National Data Guardian Standards	<b>9</b>

**Report Author: Kuljit Singh**  
**Report Version: DRAFT**  
**Report Date: 19 April 2023**



## Report Distribution

---

<b>Executive sign-off</b>	Paul Rice, Chief Digital and Information Officer
---------------------------	--

---

### Distribution

---

Jenny Pope	Head of Information Governance / Data Protection Officer
------------	--

---

Graeme Holmes	Information Governance Manager
---------------	--------------------------------

---

Matthew Horner	Director of Finance
----------------	---------------------

---

Laura Parsons	Trust Secretary
---------------	-----------------

---

Sheridan Osbourne	Corporate Governance Officer
-------------------	------------------------------

---



# 1. Executive Summary

## Introduction and background

### **Why data security and data protection issues require attention from Independent Assessors**

Data and information are a critical business asset, fundamental to the continued delivery and operation of health and care services across the UK. The Health and Social Care sector must have confidence in the confidentiality, integrity and availability of their data assets. Any personal data collected, stored and processed by public bodies are also subject to specific legal and regulatory requirements. Data security and data protection related incidents are increasing in frequency and severity; with hacking, ransomware, cyber-fraud and accidental data losses all having been observed across the Health and Social Care sector.

The need to demonstrate an ability to defend against, block and withstand cyber-attacks was amplified by the introduction of the EU Directive on security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR), now both implemented in UK law. The NIS Regulations focus on Critical National Infrastructure and 'Operators of Essential Services'; the GDPR focuses on the processing of citizens' personal data. As such, it is essential that Health and Social Care sector organisations take proactive measures to defend themselves from cyber-attacks and evidence their ability to do so in line with regulatory and legal requirements.

An additional complexity arises with the move to integrate Health and Social Care, supported by large-scale data sharing between partners across the system. Organisations need to have mutual trust in each other's ability to keep data secure and also have a requirement to take assurance from each other's risk management and information assurance arrangements.

The Data Security and Protection (DSP) Toolkit is one of several mechanisms in place to support Health and Social Care organisations in their ongoing journey to manage data security and data protection risk. Completion of an annual DSP Toolkit online self-assessment enables organisations to measure their performance against the National Data Guardian's ten data security standards, as well as supporting compliance with legal and regulatory requirements (e.g. the GDPR and NIS Directive) and Department of Health and Social Care policy.

NHS Trusts and Integrated Care Boards, as Operators as Essential Services under the NIS Regulations, are required to undergo an independent assessment of their data security and protection control environments, and to upload a completed audit report as part of their year-end Toolkit submission.

The review was conducted in accordance with the national DSP audit framework, Strengthening Assurance, now in its fourth year of operation and updated for 2022-23.

Reporting period: 01 July 2022 to 30 June 2023.



## System Objective

The objective of the Toolkit is to enable organisations to measure their performance against the National Data Guardian's ten data security standards.

## Objectives & Scope

The objective of the review is threefold:

- a) To provide to the Trust Board an overall Risk Rating and an Assurance Level in the veracity of its self-assessment
- b) to understand and help address data security and data protection risk and identify opportunities for improvement
- c) to satisfy the annual requirement for an independent assessment of the DSP Toolkit submission.

In order to meet this objective, the audit tested the sample of assertions selected by NHS Digital for assessment in the current year, focusing on the mandatory evidence questions. The results of the assessment are summarised below, in accordance with the Strengthening Assurance reporting requirements described at Appendix A. Further detail of the audit findings and recommendations are given in Section 2.

## Audit assessment

<b>Overall Assessment</b>	<b>Risk Rating</b>	<b>Moderate</b>
	<b>Assurance level</b>	<b>High</b>

Under the Strengthening Assurance framework, the Foundation Trust has attained an overall risk rating of 'Moderate' because there are no standards rated as 'Unsatisfactory', and one or none rated as 'Limited'. However, not all standards are rated as 'Substantial'. The 'High' confidence level reflects non-trivial variations between the Foundation Trust's self-assessment and that of the Independent Assessment.

## Derivation:

National Data Guardian Standard*	No of assertions assessed	Number rated Critical	Rated High	Rated Medium	Rated Low	Total Points	Overall Classification	Overall Risk Assessment	Overall Confidence in Submission
1. Personal Confidential Data	1 of 4	0	0	0	1	1	Substantial	Moderate	High
2. Staff Responsibilities	1 of 1	0	0	0	1	1	Substantial		
3. Training	1 of 4	0	0	0	1	1	Substantial		
4. Managing Data Access	2 of 5	0	0	0	2	2	Substantial		
5. Process Reviews	1 of 1	0	0	0	1	1	Substantial		
6. Responding to Incidents	1 of 3	0	0	0	1	1	Substantial		
7. Continuity Planning	2 of 3	0	0	0	2	2	Substantial		
8. Unsupported Systems	1 of 4	0	0	1	0	3	Moderate		
9. IT Protection	2 of 6	0	0	0	2	2	Substantial		
10. Accountable Suppliers	1 of 5	0	0	0	1	1	Substantial		
<b>Total</b>	<b>13</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>12</b>	<b>-</b>			

\*See Appendix B for an expanded description of each Standard

**Note:** In accordance with NHS Digital guidance, each assertion is risk assessed and a score awarded based on likelihood and impact. Full detail of the assessment and scoring methodology is in Appendix A.



## Summary of Findings

The Foundation Trust achieved and has maintained its ISO27001 certification since December 2019.

Internal Audit followed up the recommendations made in the previous BH/52/2022: Data Security and Protection Toolkit audit to identify whether they had been fully implemented, within the specified timeframes. A total of six recommendations were made in the previous report, and the position at the time of review is summarised below:

- Five recommendations have been fully implemented.
- One recommendation has been partially implemented, but is due for full implementation by the end of April 2023.

Whilst the outputs of our assessment denote an 'Overall risk assessment across all 10 NDG Standards' as 'Moderate', and an 'Assurance level based on the confidence level of the Independent Assessor in the veracity of the self-assessment' as 'High' due to only minor deviation.

Examples of best practice included:

- Data security and policies and procedures across the Foundation Trust have been reviewed and were aligned to the requirements of the Toolkit.
- Robust procedures for data security training for the SIRO and Caldicott Guardian were found to be in place, underpinned by an appropriate training needs analysis review.
- Adoption of a comprehensive approach to Data Protection by Design and Default, with a Pseudonymisation policy in place. Data protection has been adopted into wider business, alongside significant technical controls to prevent information being inappropriately downloaded.
- A Business Continuity Plan is in place, supported with a Backup process to ensure system disruption is minimised.
- An effective security monitoring control environment is in place, which meets the requirements of the DSP Toolkit. No significant data security and protection incidents have been recorded.
- The audit review identified a comprehensive process for the management of alerts received, involving the containing and investigation of these.
- The Foundation Trust has a patch management process, with a 'Deploying Windows Updates' procedure in place detailing the frequency and scope of patching. Evidence was provided which demonstrated 98.7% of servers and desktops on supported versions operating systems.
- An annual penetration test has been conducted in February 2023 by a third-party company to identify any potential cyber-security vulnerabilities. The Foundation Trust is currently awaiting the formal report of the findings.

## Direction of Travel

Improvements have been made and evidenced since the previous assessment with the Foundation Trust having ensured Data security and protection policies identified previously as requiring review have since been updated and been subject to appropriate approval. A programme of self-assessment



spot check audits has been introduced, which allow confirmation that data protection principles are followed by staff. The review confirmed that Board members were up to date with their Data Protection and Security Training. It was confirmed that the Foundation Trust has registered with the NCSC Early Warning service, which supports Microsoft Defender for Endpoints.

On the following pages, Section Two outlines one key finding and provides further context for the ratings above.

## 2. Detailed Report

### 1. Governance oversight on Patching (8.3.1)

Finding		Medium Risk	
<p>Software should receive the latest security patches to correct any known asset vulnerabilities). Those security updates / patches need to be applied in a timely fashion.</p> <p>The SIRO should have an active role in the process, and be informed when systems cannot be upgraded and the risks of using unsupported systems, and whether these risks are being treated or tolerated. The SIRO should also be notified where high risk vulnerability patches have not been applied with reasons for this within 14 days, to allow a detailed review and approval of this.</p> <p>There should be regular reporting to management or a relevant committee or group on patch status, to give them oversight of the effectiveness of the organisation's patch management activities.</p> <p>The Assertion Owner has not provided evidence effectively in line with the detailed requirements of the Toolkit. Therefore, insufficient evidence is available to confirm adherence to the assertion control.</p>			
Risk			
A lack of effective information risk management and governance may lead to increased exposure to risk and ineffective policy implementation.			
Recommendations		Risk Rating	
1.	It should be ensured that formal oversight reporting of patch status is assigned to an appropriate committee or group. Evidence should be available in future of reports being made to the responsible group.	Medium	
Management Response		Responsible Officer	Target Date
1.	Ian to provide	Ian Scott	IS/PR to agree



## Appendix A: Risk and Confidence Evaluation

### How to determine the Evidence Text Risk Rating

The DSP Toolkit Independent Assessment Provider must calculate the risk rating for each in-scope DSP Toolkit evidence text assessed as part of their DSP Toolkit review. Once the Independent Assessment Provider has assigned a likelihood and impact rating to each in-scope and assessed DSP Toolkit evidence text, the following risk rating matrix can be used to allocate a risk rating. This rating reflects the risk of the organisation being unable to meet the control objective as a result of a control failing or the absence or ineffectiveness of a control. For example, if the DSP Toolkit Independent Assessment Provider assigned a Likelihood rating of '40% - 60%' and an impact rating of 'Moderate', the risk rating for the individual evidence text would be 'Low'. The following matrix / 'look-up table' should be used to determine the Evidence Text risk ratings. Issues with a low impact and low likelihood rating should not be reported.

**Table 3. Calculation of Evidence Text Risk Rating**

[<< Return to Risk and Confidence Evaluation workflow](#)

Likelihood rating (in next 12 months)	Impact rating				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Low	Medium	High	Extreme
Likely	Low	Low	Medium	Medium	High
Moderate	Low	Low	Low	Medium	Medium
Unlikely	Very Low/ Insignificant	Low	Low	Low	Low
Rare	Very Low/ Insignificant	Very Low/ Insignificant	Low	Low	Low

### How to determine the Assertion Level Risk Rating

The DSP Toolkit Independent Assessment Provider must then exercise professional judgement to assign a risk rating at the assertion level. The Independent Assessor leverages knowledge and subject matter expertise alongside observations made during the assessment to assign each assertion a risk rating of 'Critical', 'High', 'Medium' or 'Low' based on the evidence text ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating or compensating controls in place. The Independent Assessor then uses **Table 4** to assign a score for each assertion to be used in the calculation of NDG Standard level risk.

### How to determine the National Data Guardian (NDG) Standard Risk Rating





The Independent Assessor will calculate an aggregate score and classification for each NDG Standard - i.e. the overall NDG Standard risk rating that will appear in the Executive Summary of the DSP Toolkit Independent Assessment Provider report. That is, the Executive Summary reporting will be at the NDG standard level; providing 10 'scores'; one for each standard. This guide also outlines how an overall risk rating score can be calculated. It is understood that this will be an expectation of key stakeholders to provide an overall risk rating though it should be noted and understood that abstracting scores to a high level and using aggregate or average scores can be very misleading as they can sometimes mask significant or critical issues at the lower levels; i.e. at the assertion level. For some NDG standards there may be multiple assertions in the scope of the independent assessment and for some NDG standards there may only be one assertion in scope. The NDG Standard risk rating is determined by calculating the mean of the total number of assertion level points per NDG Standard. For example, a DSP Toolkit Independent Assessment Provider who assessed 8 DSP Toolkit Assertions aligned to NDG Standard One, may rate 5 assertions as Critical, 2 as High and 1 as a Medium. Using Table 4 below, this gives the DSP Toolkit Independent Assessment Provider a total of 223 points (200 for Critical findings, 20 for High and 3 for Medium = 223 points). These figures should be divided by the number of assertions reviewed and rounded to the nearest one decimal place. In this instance 8 assertions will yield a mean points per assertion of 28 ( $223 \div 8 = 27.9$  rounded to one decimal place). Table 5 should then be used to determine the overall NDG Standard Risk Rating, in this instance it would provide an 'Unsatisfactory' classification. This will be done for each NDG standard to support an overall risk rating.

**Table 4. Points corresponding to Assertion Risk Ratings**

Rating	Points for each Assertion
Critical	40
High	10
Medium	3
Low	1

**Table 5. Calculation and Assignment of the NDG Standard Risk Ratings**

[<< Return to Risk and Confidence Evaluation workflow](#)

Overall NDG Standard Risk 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 is to be used (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



### How to determine the Overall Risk Assurance Rating

Once the Independent Assessment Provider has calculated the risk assurance rating for each Standard the following principle can be used to allocate the overall risk rating.

The DSP Toolkit Independent Assessment Provider should calculate the overall risk rating of the organisation's data security and protection controls. Table 6 below allows the independent assessment provider to conduct this calculation.

**Table 6. Determination of Overall Risk Assurance Rating**

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'

### How to determine the Overall Confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission

Once the Independent Assessment Provider has completed the fieldwork and calculated the ratings for assertions, for each of the 10 NDG standards the veracity of the organisation's DSP Toolkit self-assessment submission should be determined by comparing the independent assessment findings with the self-assessment. The following definitions should be used for aiding the decision of applying a confidence-level. It is noted that the evidence available to the Independent Assessment Provider may differ or may have changed from the evidence in place at the time of the self-assessment. Furthermore, the self-assessment may not have much evidence. The Independent Assessor will need to take that into consideration when determining the confidence level and when writing the report and putting it into context. It may be possible so the self-assessment and independent assessment may differ but not necessarily due to a lack of veracity or honesty in the self-assessment.

**Table 7. Determination of confidence-level in the veracity of the organisation's self-assessment / DSP Toolkit submission**

Level of deviation from the DSP Toolkit submission and assessment findings
<p><b>High level of deviation</b> - the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment</p> <p>For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual NDG standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'.</p>
<p><b>Medium level of deviation</b> - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment</p> <p>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.</p>
<p><b>Low level of deviation</b> - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment</p>



## Appendix B: The Ten National Data Guardian Standards

National Data Guardian Standard	Description
<b>1. Personal Confidential Data</b>	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
<b>2. Staff Responsibilities</b>	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
<b>3. Training</b>	All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.
<b>4. Managing Data Access</b>	Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
<b>5. Process Reviews</b>	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
<b>6. Responding to Incidents</b>	Cyber-attacks against services are identified and resisted and security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
<b>7. Continuity Planning</b>	A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.
<b>8. Unsupported Systems</b>	No unsupported operating systems, software or internet browsers are used within the IT estate.
<b>9. IT Protection</b>	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually
<b>10. Accountable Suppliers</b>	IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

