Report to:	**Public Board of Directors**	**Agenda item:**	**17**
Date of Meeting:	**22nd July 2024**		

Title of Report:	**SIRO Data Security Protection Toolkit Report July 2024**
Status:	**For Approval**
Board Sponsor:	**Jon Lund, Interim Chief Finance Officer on behalf of Spencer Thorn, Acting Senior Information Responsible Officer (SIRO)**
Author:	**Graeme Temblett-Willis**
Appendices	**Appendix 1 – DSPT status and certificate of completion June 2024.**

1. Executive Summary

The purpose of this report is to update the Committee on the status of Information Security and Governance for the Trust and with reporting on the annual Data Security Protection Toolkit (DSPT) for the period July 2023 to June 2024.

The report covers relevant compliance and regulatory controls that the Trust adheres to and is working to improve in an ever-changing security threat environment.

The appendices are to provide an extra layer of detail for this Committee.

The final submission for the DSPT for 2023-24 has now been submitted following approval from the Non Clinicla Governance Committee and is the detail provided to NHS England to show final completion of this assessment. This is then available to the public and partners to show the Trust meets the standards of compliance in the management of patient data, clinical systems and technology used by the organisation less the granular detail that sits behind the assessment.

2. Summary

1. ***Annual Data Security Protection Toolkit (DSPT).***

The KPMG DSPT internal audit has concluded and involved a deep dive into several areas not previously assessed. The detail that has been explored are:

a) The organisation has a framework in place to support Lawfulness, Fairness and Transparency
b) Staff contracts set out responsibilities for data security.
c) Staff have appropriate understanding of information governance and cyber security, with an effective range of approaches taken to training and awareness.
d) Your organisation engages proactively and widely to improve data security and has an open and just culture for data security incidents.
e) You closely manage privileged user access to networks and information systems supporting the essential service.
f) Process reviews are held at least once per year where data security is put at risk and following DS incidents.
g) All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.
h) Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.
i) You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.
j) A penetration test has been scoped and undertaken.

k) You securely configure the network and information systems that support the delivery of essential services.
l) The organisation is protected by a well-managed firewall.
m) Basic due diligence has been undertaken against each supplier that handles personal information.

There are challenges in a number of these assertions for the organisation and they must be considered in relation to risk, resource and time to deliver. The challenges that are involved in the assessment and require significant resource centre on the management of our network and information system vulnerabilities that are becoming more complex and the lack of a SIEM (Security Incident and Event Monitoring) tool that enables such vulnerabilities to be monitored out of hours poses a significant risk to the Trust and has been demonstrated in the recent cyber attack on the Trust firewall which has been discussed previously at this Committee.

The assertions that were included in this year's audit total 59 out of the 108 mandatory assertions that make up the full DSPT annual assessment. The remaining assertions that have not been assessed this year are assessed via a process of collection and engagement with the relevant staff across the Trust including medical records, coding, medical device management, networks, cyber, service desk leads, EPRR and procurement. The SIRO or Deputy SIRO are then provided with a full explanation of each of the 10 data security standards prior to final submission.

The final KPMG internal audit report has been given a rating of ***Significant assurance with minor improvement opportunities (Amber / Green)***.
The improvement opportunities that are detailed in the final report relate to the creation of new policies not previously published or required under UK GDPR but relate more to cyber assurance and the management process of medical devices as there is no formally documented plan for protecting devices that are natively unable to connect to the Internet. (This applies to any device (managed internally or by a third party) that does not have a route to/from the Internet, such as air-gapped networks or stand-alone devices, for example an MRI Scanner).

Areas of good practice identified by the internal audit included:

- The Trust provides a specific privacy notice tailored for children and young adults, which is an easy-to-understand version of the privacy notice for adults.
- Mandatory Information Governance and Data Security training is conducted annually for all staff, with compliance tracked through an Organisational Compliance Report.
- The access privileges to system logs in the central logging management system are strictly controlled, limiting access to authorised personnel only.
- The Trust has established a structured process for reporting and investigating data security incidents, ensuring timely resolution and mitigation.
- Key operational services are documented and categorised by priority levels, facilitating resource allocation and management.
- Secure infrastructure measures, including a frequent patching schedule, vulnerability checks, and monitoring alerts, are implemented to mitigate risks.
- A Mobile Device Management (MDM) solution is in place to ensure the security

of mobile and tablet devices across the Trust.

- Documented standards for end-user devices include monthly patching schedules, encryption, and user account management, enhancing security measures for provisioned devices.
- Changes to firewall rulesets require submission of detailed change requests to the service owner, ensuring planning and risk mitigation.

The DSPT assessment has evolved over the last three years and is now information security focused not simply an Information Governance exercise. It ensures the Trust moves towards not only NHS England standards but also best practice across the healthcare industry taking other frameworks as an aide to improve our assurance and compliance with the UK regulatory landscape.

In the next annual DSPT assessment this will be aligned and follow the CAF (Cyber Assessment Framework) that is provided by the NCSC (National Cyber Security Centre) who have worked with NHS England to ensure the healthcare sector can be more resilient into the future with the ever-increasing threat of cyber and security attacks.

The interim Deputy CDIO and DPO (Data Protection Officer) is attending a series of events to ensure this level of compliance is understood in granular detail. This will be relevant particularly as the Acute collaboration in the digital space moves forward. Such collaboration should be mindful of the need to manage the statutory requirements regarding data privacy and Network and Information System (NIS) security so that no single Trust is compromised.

2. ICO Incidents reported.

There have been three reports of confidentiality breach made directly to the ICO (Information Commissioners Office) which have been investigated with one concluded and no further action or involvement required from the ICO. The second continues to be investigated and relates to the loss of a patient list stolen from a staff members folder whilst in a public place. This has been reported to the police and ICO with further details on their progress awaited.

The third report relates to the ongoing cyber-attack in London and the potential for data belonging to the Trust being involved in the ransomware attack in June. (This has been covered ahead of this section).

The Board will be updated on all incidents once the ICO case manager has returned with their view of the investigation undertaken locally.

There has been a total of 164 Information Governance reported incidents during the period July 2023 – May 2024 none causing significant risk of harm to patients or staff. Learning is provided as feedback and training offered by the IG team for those areas identified as having a recurring trend of incidents. Many incidents relate to letters being sent to wrong recipient and a on closure investigation into this increasing trend has been due to staff pressures and incorrect choice of patient on the relevant clinical application.

Further training and awareness has been provided to the clinical administration leads in the Divisions and it is hoped that the incidents will reduce over the coming months.

Incident statistics are reported monthly to the ISG (Information Security Group) and it should be noted that there is a high level of awareness in relation to patient confidentiality and this is evidenced by the number of BAU queries that the IG team receive in relation to seeking advice and guidance which was approximately 1200 email queries for July 2022- June 2023 but now has reached in excess of 1600 for 2023-24 period plus general phone call queries which are managed by just two members of staff. Thie team now also respond to Information Governance matters that relate to Sulis.

3. **Freedom of Information (FOI)**

FOI requests have increased again as shown below:

Freedom of Information requests have increased again as shown below: There have been 354 requests received for the time frame from 1st January 2024 – 3rd May 2024 which is 57% compliance.

For reference, please see the statistics for the same reporting period for previous years below.

Numbers received = 354 to date
Numbers received = 288 - 2023
Numbers received = 223 – 2022
Numbers received = 219 – 2021
Numbers received = 211 - 2020

The level of requests is a challenge to both the FOI coordinator and to the organisation to complete beyond the normal daily tasks. Currently the Trust is well below the required 90% target set by the ICO.

The lack of an automated FOI process hinders the ability to drive increased compliance and discussions continue across the AHA to find a solution that will benefit all sites. There is a risk that not being able to meet the statutory response could result in enforcement action in the form of notices and penalties could materialise. The ICO have taken action against other public authorities recently for the lack of responding to FOI requests as can be evidenced in the following link https://ico.org.uk/action-weve-taken/information-notices/ .

The Information Security Group is committed to improving the level of compliance for FOI requests and provides monthly reports on progress in achieving this and further updates will be provided to this Committee. The following is now being put in place to improve the compliance:

- *Training programme – provide training to key staff identified as responsible leads for completing departmental FOI’s*

- *Increased data analysis – identifying trends of non-compliance and areas that are falling behind in completion more promptly and provide KPI trackers to improve compliance.*
- *Review internal processes – improving internal processes and identifying blockages in the system will reduce response times.*
- *Increase proactive disclosure – by publishing more information widely on the Trust external website can lead to signposting of previously requested data thereby reducing the burden on staff and the FOI process.*
- *Improved FOI assessment – early identification of exemptions that can be applied and data previously requested that has been provided to other requestors will improve performance.*
- *Utilize technology – the new IT Service Desk system, Halo, is being scoped as to whether this can help automate or semi-automate the FOI process.*
- *Increased audits – introduction of regular auditing of FOI to be introduced and reported to ISG and via the PRM process to monitor and evaluate progress.*

3. Recommendations (Note, Approve, Discuss etc)

- Request to note and approve the report.

4. Care Quality Commission Outcomes (which apply)

The DSP Toolkit compliance helps demonstrate compliance with Regulation 17 – Good governance.

5. Legal / Regulatory Implications (ICO)

UK General Data Protection Regulation (GDPR) / Data Protection Act 2018

The UK GDPR is applicable to any organisation that processes personal data – public, private and voluntary sectors. The key themes of the new legislation are more rights for individuals in relation to how their personal data is processed and more obligations for organisations that are processing personal data, whether of staff or patients / service users.

An updated Data Protection Bill was expected to have been passed earlier this year (2024) but has failed to reach the deadline prior to the call of the General Election. There were aspects of the Bill that changed some approaches to records of processing and risk assessments, as well as having a tiered approach to penalties and fines on the UK GDPR. If the Bill is resurrected at the new term of Government that may not be until the end of the summer recess this will be reported back to this Committee.

The Freedom of Information Act (FOIA)

Responding to requests under the Freedom of Information Act (2000) has been the responsibility of the Information Governance Team. The service is administered by one 1 WTE member of staff and managed by the Information Governance Manager. FOI activity is monitored by the Information Governance Group and each request has Executive sign off by the Trust Secretary. The FOI Act states that for a request to be compliant with the legislation then the information must be provided and responded to within 20 working days.

Information Governance Data Incidents

The Trust reports all serious Information Governance incidents to the ICO by using the online NHSD DSPT incident reporting tool, which is the agreed standard in relation to data breaches and incidents. Incidents that are required to be reported to the ICO must be made within 72 hours of being discovered.

All incidents are triaged by the IG Team and any that require escalation are done so through the DSPT mechanism.

Networking and Collaboration

Internally, the Deputy CIO (interim) / DPO and IG Team are represented at various groups and committees on both ad hoc and regular basis.

Externally, these roles contribute to the West of England Strategic Information Governance Network (SIGN), the WiSC (Wiltshire information Sharing Charter), WIGF (Wessex Information Governance Forum) and the BSW ICS Cyber Technical Design Authority, providing guidance and advice as the Data Protection Officer for the ICS Local Workforce Administration Board (LWAB). The DPO has also been key to the governance structure for the N365 rollout and other regional initiatives including radiotherapy, radiology, and cancer networks agreements. The Trust DPO (Deputy CDIO) is also the IG lead and SME for the West of England Imaging Network.

6. NHS Constitution

This report shows that the Trust is committed to maintaining patient confidentiality and patient’s right to privacy, as well as complying with the Data Protection principles.

7. Equality and Diversity

The control of data in relation to the organisation is unbiased and non-discriminatory respecting the rights and freedoms of all staff and patients alike.

8. Communication

NA.

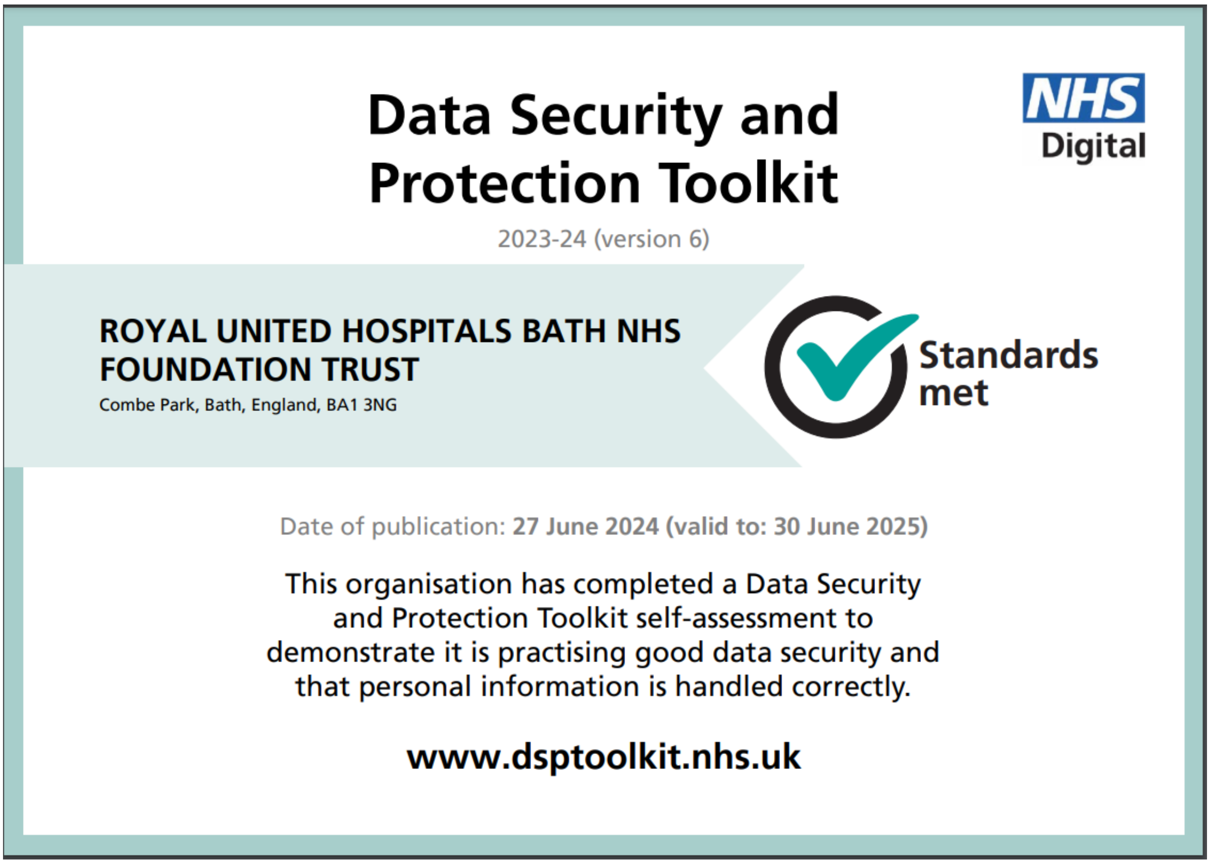
9. References to previous reports

DSPT update previously considered at Non Clinical Governance Committee, June 2024

10. Freedom of Information

Public

Appendix 1 – DSPT status June 2024



Data Security and Protection Toolkit

2023-24 (version 6)

NHS Digital

ROYAL UNITED HOSPITALS BATH NHS FOUNDATION TRUST

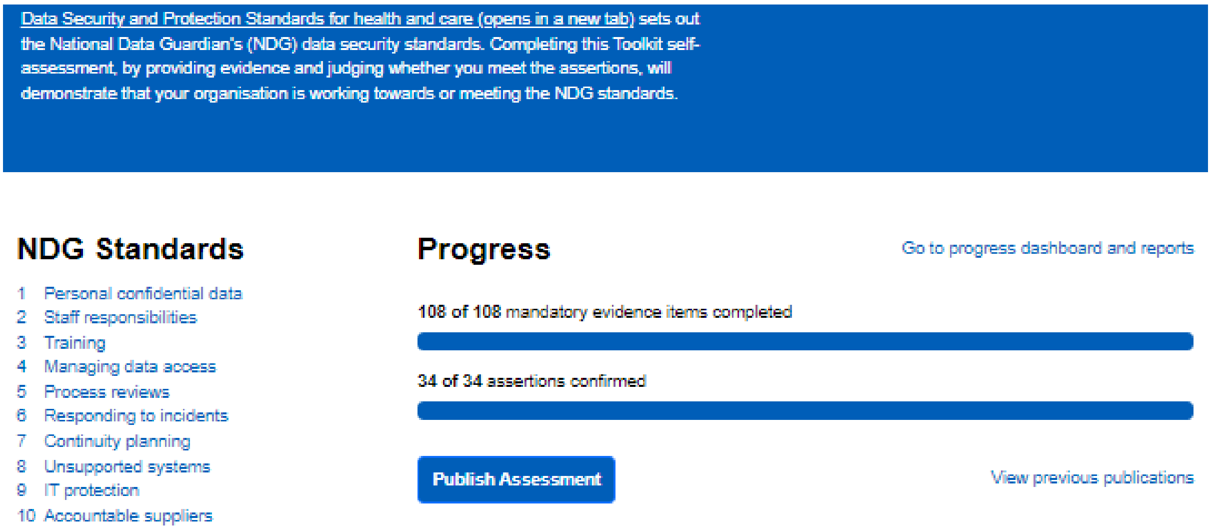
Combe Park, Bath, England, BA1 3NG

Standards met

Date of publication: **27 June 2024 (valid to: 30 June 2025)**

This organisation has completed a Data Security and Protection Toolkit self-assessment to demonstrate it is practising good data security and that personal information is handled correctly.

www.dsptoolkit.nhs.uk



Data Security and Protection Standards for health and care (opens in a new tab) sets out the National Data Guardian's (NDG) data security standards. Completing this Toolkit self-assessment, by providing evidence and judging whether you meet the assertions, will demonstrate that your organisation is working towards or meeting the NDG standards.

NDG Standards

1 Personal confidential data
2 Staff responsibilities
3 Training
4 Managing data access
5 Process reviews
6 Responding to incidents
7 Continuity planning
8 Unsupported systems
9 IT protection
10 Accountable suppliers

Progress

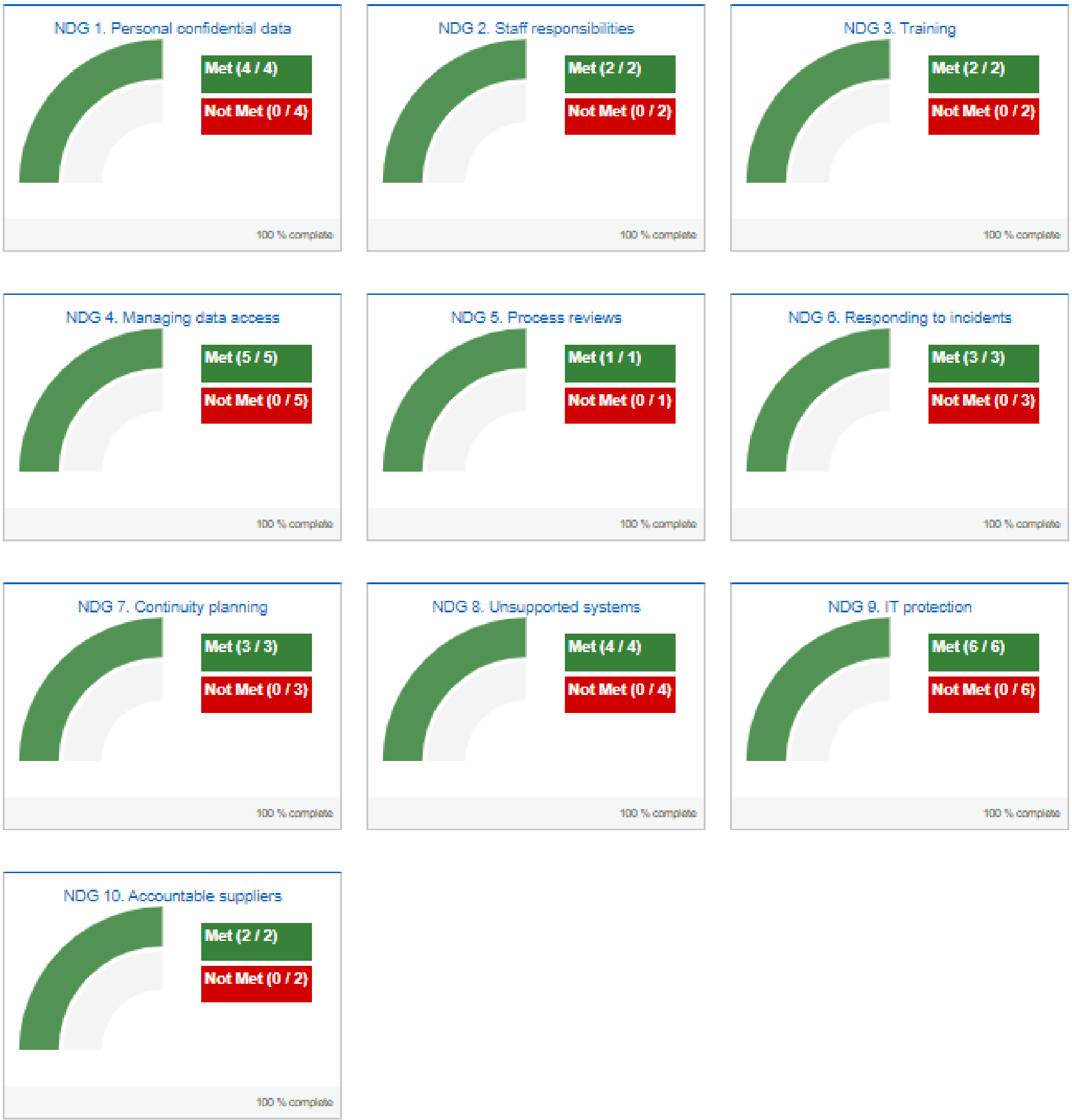
Go to progress dashboard and reports

108 of 108 mandatory evidence items completed

34 of 34 assertions confirmed

National Data Guardian Standards

The National Data Guardian (NDG) standards have been calculated for your organisation based on the responses provided in your organisation profile.



NDG 1. Personal confidential data
Met (4 / 4)
Not Met (0 / 4)
100 % complete

NDG 2. Staff responsibilities
Met (2 / 2)
Not Met (0 / 2)
100 % complete

NDG 3. Training
Met (2 / 2)
Not Met (0 / 2)
100 % complete

NDG 4. Managing data access
Met (5 / 5)
Not Met (0 / 5)
100 % complete

NDG 5. Process reviews
Met (1 / 1)
Not Met (0 / 1)
100 % complete

NDG 6. Responding to incidents
Met (3 / 3)
Not Met (0 / 3)
100 % complete

NDG 7. Continuity planning
Met (3 / 3)
Not Met (0 / 3)
100 % complete

NDG 8. Unsupported systems
Met (4 / 4)
Not Met (0 / 4)
100 % complete

NDG 9. IT protection
Met (6 / 6)
Not Met (0 / 6)
100 % complete

NDG 10. Accountable suppliers
Met (2 / 2)
Not Met (0 / 2)
100 % complete