**Audit and Risk Assurance Committee (ARAC)**

Date: 19 October 2023

Paper reference: AUD 33/23

Agenda item: 9.

Author: Sam Mortimer

2023-2024 Data Security and Protection Toolkit (DSPT) Overview

Purpose of paper

1. To provide ARAC with an overview of changes to the 2023-2024 Data Security and Protection Toolkit.
2. To make ARAC aware of key DSPT role changes in HTA.

Decision making to date

1. New DSPT 2023-2024 standards and guidance published on 30 August 2023.

Action required

1. ARAC is asked to note the main changes to the 2023-2024 Data Security and Protection Toolkit and the impact on HTA.
2. ARAC is asked to note key DSPT role changes.

Background

1. The Data Security and Protection Toolkit is an online self-assessment tool maintained by the NHS that allows organisations to measure their performance against the National Data Guardian’s 10 data security standards.
2. The HTA, has been completing DSPT assessments since 2019 because we have access to NHS patient data and systems.
3. As an ALB, HTA is classed as a Category 1 organisation, and we are required to provide assurance that we are practising good data security, and that personal information is handled correctly against a pre-determined set of assertions.
4. The key deadlines for 2023 – 2024 are, 29 February 2024 for the baseline assessment and 30 June 2024 the final assessment.

Changes to the 2023-2024 DSPT

1. There are minimal changes for 2023-24. The biggest change relates to data security awareness. This will be an audited requirement for 2023/24.
2. Key national standard changes are provided below:

**Training**

The staff training requirement has been changed to allow larger organisations more flexibility around delivery.

New assertions:

3.1.2 Your organisation’s defined training and awareness activities are implemented for and followed by all staff.

3.1.3. Provide details of how you evaluate your training and awareness activities.

3.2.2 Actions are taken openly and consistently in response to information governance and cyber security concerns.

3.2.3 Your information governance and cyber security programme is informed by wide and representative engagement with staff.

Removed assertions:

3.3.2 The organisation has appropriately qualified cyber security specialist staff and/or service.

3.3.4 All board members have completed appropriate data security and protection training.

These assertions are no longer applicable for Category 1 organisations:

3.3.1 Staff with specialist roles receive data security and protection training suitable to their role.

3.4.1 Leaders and board members receive suitable data protection and security training.

**Managing data access**

Multi-factor authentication improvements have been included to reflect the updated policy.

Reworded assertion:

4.5.3 Multi-factor authentication is enforced on all remote access and privileged user accounts on all systems, with exceptions only as permitted by the national MFA policy.

**Responding to incidents**

Reworded assertion and guidance:

6.1.1 Data security and protection incidents are reported appropriately and by a full range of staff groups. Incidents and near misses to be by staff groups to be included in reporting.

**Unsupported Software and Operating Systems**

Removed assertion:

8.1.3 All software and hardware has been surveyed to understand if it is supported and up to date.

Both of these assertions have been updated to include for alternative controls:

8.3.7 95% of your organisation’s server estate and 98% of your desktop estate are on supported versions of operating systems. Where this is not possible, there is a SIRO approved plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.

8.4.2 All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted, regularly reviewed and signed off by the SIRO.

Update guidance:

8.2.1 Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.

8.4.3 You maintain a current understanding of the exposure of your hardware and software to publicly known vulnerabilities.

**IT Protection**

Removed assertion:

9.2.2 The date the penetration test and vulnerability scan was undertaken. A penetration test has been scoped and undertaken.

**Information governance templates**

NHS England has launched a new suite of templates in August 23. The suite covers templates for Data Protection Impact Assessments, Data Sharing and Processing Agreements, Information Assets & Flows Registers and Privacy Notices. Templates are available [here](https://transform.england.nhs.uk/information-governance/guidance/universal-ig-templates-faqs/). Use of these templates are not mandatory but are recommended for consistency.

DSPT Changes 2024- 2025

1. NHSE plan to replace elements of the existing DSPT content with the Cyber Assessment Framework (CAF) in 2024. This will allow Category organisations more flexibility (with some must-do requirements) to decide how they deliver an outcome rather than the current, more prescriptive approach of the DSP Toolkit.

Changes to key DSPT roles

1. Tom Skrinar, the Director of Resources, has taken on the role of Senior Information Risk Owner (SIRO) since September 2023.
2. Nicholas Taylor, Records Management and Information Governance Lead is responsible for Information Governance, Data Protection and DSPT
3. Louise Dineley, Director of Data, Technology and Development, continues in the role of Caldicott Guardian.