|  |  |
| --- | --- |
| **Report to:** | Humber and North Yorkshire Integrated Care Board |
| **Date of Meeting:** | 8th January 2025 |
| **Subject:** | **Information Governance – Data Security & Protection Toolkit – Updates & Audit** |
| **Director Sponsor:** | Karina Ellis – Executive Director of Corporate Affairs |
| **Author:** | Hayley Gillingwater – Senior Information Governance Manager |

|  |  |
| --- | --- |
| **Agenda Item No:** | **13** |



|  |
| --- |
| **STATUS OF THE REPORT:**  Approve  Discuss  Assurance  Information  A Regulatory Requirement |

|  |
| --- |
| **SUMMARY OF REPORT:**  The ICB must complete a Data Security and Protection Toolkit (DSPT) annual self-assessment and submit this to NHS England. This year the data security and protection toolkit has changed to adopt the National Cyber Security Centre’s Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.  Organisations will self-assess their level of compliance against each outcome using the indicators of good practice as a guide.  The process of submitting assessments to NHS England will not change.  National assurance will continue to be based on organisations commissioning independent audits of their self-assessments, complemented by national sampling audits.  There is a total of 47 outcomes in the CAF-aligned DSPT, which will all be assessed over a multi-year period. Each year, a selection of outcomes from across the five objectives will be tested by independent assessment providers. NHSE will mandate a common core set of outcomes to be assessed for all organisations that undertake the CAF-aligned DSPT, while a further four outcomes will be selected by individual organisations. These outcomes should be approved by the Board of each organisation (or person with delegated responsibility), and will reflect areas of concern that warrant additional assurance over the controls in place during that audit period.  The Senior Information Governance Manager and Senior Information Risk Owner have selected the additional 4 outcomes to be audited these will be detailed in the report below. The Board are asked to approve these areas for audit.  **RECOMMENDATIONS:**  Members are asked to:   1. Note the changes to the Data Security & Protection Toolkit for 2024-25 2. Approve the additional 4 outcomes suggested for audit. 3. Support the Senior Information Governance Manager to raise awareness of the changes within the ICB. |

|  |
| --- |
| **ICB STRATEGIC OBJECTIVE** |

|  |  |
| --- | --- |
| Leading for Excellence | ☒ |
| Leading for Prevention | ☒ |
| Leading for Sustainability | ☐ |
| Voice at the Heart | ☐ |

|  |
| --- |
| **IMPLICATIONS** |

|  |  |
| --- | --- |
| Finance | There may be financial implications for the ICB due to some of the additional requirements in the new DSPT. |
| Quality | No adverse implications identified. |
| HR | No adverse implications identified. |
| Legal / Regulatory | All organisations that have access to NHS patient data and systems must use the data security & protection toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.  Independent Providers who have been designated Operators of Essential Service and IT Suppliers must ensure that their audit provider follows the mandated scope which for this year is set out in the DSPT Independent Assessment Guide. |
| Data Protection / IG | As above. |
| Health inequality / equality | No adverse implications identified. |
| Conflict of Interest Aspects | No adverse implications identified. |
| Sustainability | No adverse implications identified. |

|  |
| --- |
| **ASSESSED RISK:** Risks associated with failure to meet the standards of the DSPT:   * a removal of services (e.g. ICB not achieving could mean the ICB not receiving national data flows) * Increased risk of financial impact/reputational damage in the event of an ICO reportable incident, as the ICO will take into account any non-compliance with DSPT as part of its assessment of a breach * breach of contracts/ data sharing agreements where we have confirmed DSPT standards are met. |

|  |
| --- |
| **MONITORING AND ASSURANCE:**  The external audit of the data security and protection toolkit will provide assurance that standards are being met. |

|  |
| --- |
| **ENGAGEMENT:**  Not applicable. |

|  |
| --- |
| **REPORT EXEMPT FROM PUBLIC DISCLOSURE** No ☒ Yes ☐ |
| If yes, please detail the specific grounds for exemption. |

**Data Security & Protection Toolkit Updates & Audit Requirements**

1. **INTRODUCTION**
   1. In September 2024 the DSPT changed to adopt the National Cyber Security Centre’s Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance. The Goal of the CAF is to set out broad principles to drive good decision making, rather than a “compliance checklist” of good practices.

Organisations will self-assess their level of compliance against each outcome using the indicators of good practice as a guide. The process of submitting assessments to NHS England will not change. National assurance will continue to be based on organisations commissioning independent audits of their self-assessments, complemented by national sampling audits.

1. **BACKGROUND**

The new toolkit aims to emphasise good decision making over compliance, with better understanding and ownership of information risks at the local organisation level, where those risks can be most effectively managed. They aim to support a culture of evaluation and improvement, as organisations will need to understand the effectiveness of their practices at meeting the desired outcomes, and expend effort on what works, not what ticks a compliance box. It also aims to create opportunities for better practice, by prompting and enabling organisations to remain current with new security measures to meet new threats and risks.

The first step for all organisations will be to carry out a scoping exercise to understand, and document, what their essential functions are as many of the outcomes reference the measures that need to be in place to ensure these essential functions are safe/secure and can be brought back online in the correct way/order if an incident occurs.

The CAF Aligned DSPT is split into Objectives, Principles & Outcomes covering the following areas:

Objective A Managing Risk

Objective B Protecting against cyber attack and data breaches

Objective C Detecting cyber security events

Objective D Minimising the impact of incidents

Objective E Using and sharing information appropriately

Organisations will need to assess themselves against 47 outcomes across the 5 Objectives, each outcome is assessed against a set of statements that fall into categories of “Not Achieved”, “Partially Achieved” or “Achieved”. NHSE have determined the expected achievement level for each outcome to enable an organisation to meet Standards Met. All statements within a category must apply in order to achieve that outcome, if any of them are not then the lower category must be selected. There are 6 Outcomes where organisations can assess themselves as “Not Achieved” this year, however as part of the assessment it is expected that a plan is submitted to move to the next category up in future years.

Whilst expectations for cyber security and IG controls remain at a reasonably comparable level to the previous DSPT assessment, 12 of the Outcomes have an increase in requirements to achieve the NHSE minimum achievement level to achieve Standards Met.

New ways of working will mean, for this year at least, an increase in the resource needed to complete, both from within Cyber & IG teams and from the wider teams within each organisation, for the ICB this includes EPRR/Corporate/Comms/HR/Asset Owners. NHSE have already indicated that in future years the expected achievement levels will increase, this could again have an impact from a resource perspective and from a financial perspective if additional/different tools are required to enable organisations to meet the minimum achievement level.

#### ASSESSMENT

#### A selection of outcomes from across the five objectives will be tested by independent assessment providers. NHSE will mandate a common core set outcomes to be assessed for all organisations that undertake the CAF-aligned DSPT, while a further four outcomes will be selected by individual organisations.

**Mandatory Outcomes**

* **A2.a Risk management process**  
  Your organisation has effective internal processes for managing risks to the security and governance of information, systems and networks related to the operation of your essential function(s) and communicating associated activities. This includes a process for data protection impact assessments (DPIAs).
* **A4.a Supply chain**  
  The organisation understands and manages security and IG risks to information, systems and networks supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.
* **B2.a - Identity verification, authentication and authorisation**  
  You robustly verify, authenticate and authorise access to the information, systems and networks supporting your essential function(s).
* **B4.d - Vulnerability management**  
  You manage known vulnerabilities in your network and information systems to prevent adverse impact on your essential function(s).
* **C1.a Monitoring coverage**  
  The data sources that you include in your monitoring allow for timely identification of security events which might affect the operation of your essential function(s).
* **D1.a - Response plan**  
  You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of your essential function(s) and covers a range of incident scenarios.
* **E2.b – Consent**  
  You have a good understanding of requirements around consent and privacy, including the common law duty of confidentiality, and use these to manage consent.
* **E3.a Using and sharing information sharing for direct care**  
  You lawfully and appropriately use and share information for direct care.

**The Senior Information Governance Manager and the Senior Information Risk Owner have selected the below additional 4 outcomes:**

* **E2.a Managing data subject rights under UK GDPR**

You appropriately assess and manage information rights requests such as subject access, rectification and objections.

*As a result of complaints and reports to the ICO the SAR Team has undertaken significant work to strengthen the process and we have produced additional guidance for staff. In the event of any further complaints to the ICO it would be useful to have external assurance from our auditors on the process to present as part of any investigation that may arise.*

* **B3.d Mobile data**

You have protected data important to the operation of your essential function(s) on mobile devices.

*Mobile Device Management (MDM) rollout has been completed on all mobile devices; however, we are now moving to a new mobile provider and as a result staff will need to move from the existing MDM system to a new one. Guidance on the new rollout has been issued to staff but we are aware IT have been experiencing issues with this process and we would like external assurance that MDM has been appropriately installed on all ICB mobile devices.*

* **B3.e Media/equipment sanitisation**

Before reuse and / or disposal you appropriately sanitise devices, equipment and removable media holding data important to the operation of your essential function(s).

*As part of the transition to the new IT provider a number of devices will need to be reimaged or potentially disposed of, the ICB would like assurance that this is being managed appropriately***.**

* **C2.a System abnormalities for attack detection**

You define examples of abnormalities in system behaviour that provide practical ways of detecting malicious activity that is otherwise hard to identify.

*As above with NECS taking on responsibility for a number of systems and networks that have previously been managed by other providers we would like assurance that they have the ability to detect any issues or abnormalities.*

##### CONCLUSION

* 1. There are significant changes to the format and requirements of the Data Security & Protection Toolkit for the 24-25 submission (June 2025). The auditors are liaising with the Senior Information Governance Manager and have asked for confirmation of the additional 4 outcomes to be audited. The suggested additional outcomes and rationale are detailed above at section 3.

1. **RECOMMENDATIONS**
   1. Members are asked to:
2. Note the changes to the Data Security & Protection Toolkit for 2024-25
3. Approve the additional 4 outcomes suggested for audit.
4. Support the Senior Information Governance Manager to raise awareness of the changes within the ICB

**Annex A – CAF aligned DSPT Requirements**

