NHS
North East
Ambulance Service
NHS Foundation Trust

Public Trust Board of Directors Meeting No.4 2026/27			
Date of Meeting:	Thursday 19 November 2026		
Executive Sponsor:	Paul Nicholson, Director of Technology and Information	**Author(s):**	Daniel Malone, Cyber Security and Technical Implementation Manager
Title:	**Cyber Security Assuracne Report**		
Paper Type:	For Decision ☐	For Assurance ☒	For Information ☐
Paper Status:	Public ☒	Private ☐	Internal ☐
Purpose:	This report provides an assessment of the Trust's position against the expectations set out in the NHS England letter. It describes the Trust's current areas of strength, identifies opportunities for further improvement and explains the likely organisational, technical and workforce implications of future Data Security and Protection Toolkit and Cyber Assessment Framework requirements. The report also seeks to reinforce the central message from NHS England that cyber security is an organisational risk, rather than solely an IM&T responsibility, and requires sustained executive leadership, effective governance and participation across clinical, operational and corporate services.		
Recommendation:	The Board is asked to: 1. **Note** the contents of the NHS England letter and the increasing national expectations for Board and executive assurance over cyber security risk. 2. **Take assurance** that the Trust continues to achieve the NHS Data Security and Protection Toolkit standard of Standards Met and has established governance, technical, monitoring, incident response and organisational resilience arrangements. 3. **Note** that DSPT compliance represents the current minimum mandatory baseline and does not constitute assurance that all Cyber Assessment Framework outcomes are fully achieved, or that cyber security controls have reached the same level of maturity across the wider organisation. 4. **Note** that future DSPT and CAF requirements will require sustained year-on-year investment, changes to existing infrastructure and operating models, additional organisational capacity and, in some cases, redesign or replacement of legacy systems and processes. 5. **Note** the ongoing review of the IM&T operating model and future departmental structure so that the Trust has sufficient architectural, technical, cyber security, governance, assurance and implementation capability to meet forthcoming requirements. 6. **Note** that all proposed new systems, technology-enabled services and significant changes to existing systems follow the Trust's gateway process, with appropriate technical, cyber security, Information Governance and operational involvement before products or solutions are selected. 7. **Note** the contribution of the Emergency Preparedness, Resilience and Response function as a significant component of the Trust's cyber incident response and organisational resilience arrangements.		

Previously Considered by:	Executive Management Group, Information Technology and Security Group (ITSG) and Audit and Risk Committee.
Onward submission to:	N/A

Please indicate how paper links to the following key considerations:

Strategic Objectives:	Data-Driven Clinical Interventions & Left Shift ☐		Define & Enhance Quality at NEAS ☒		Improve ARP Performance ☐
	Improve Staff Experience & Maximise Contribution ☐		Improve Long-Term Sustainability of the organisation ☒		Enable Analogue-to-Digital Transition ☒
System Triple Aims:	Better health outcomes ☒		Better experiences for people ☐		Better use of resources ☒
Trust Values:	Compassion ☐	Accountability & Responsibility ☒	Respect ☐	Excellence & Innovation ☒	Proud to Make a Difference ☒
CQC Quality Statements:	Safe ☒	Effective ☒	Caring ☒	Responsive ☐	Well-Led ☒

NHS
North East
Ambulance Service
NHS Foundation Trust

Executive Summary

On 10 June 2026, NHS England issued a letter asking NHS Boards and executives to assure themselves that cyber security risks are being managed effectively and that clear, sustained programmes of improvement are in place. The letter highlights increasing cyber threats arising from geopolitical events, evolving technology and greater reliance on digital services. It also makes clear that the consequences of a cyber attack affect the whole organisation, rather than only its digital or IT functions.

NEAS continues to achieve the NHS Data Security and Protection Toolkit (DSPT) standard of Standards Met. This provides assurance that the Trust has implemented the minimum cyber security and information governance controls currently required by NHS England. The DSPT is aligned with the principles of the National Cyber Security Centre's Cyber Assessment Framework (CAF), although it does not currently require organisations to fully achieve all CAF outcomes or maturity expectations.

The Trust has significant existing strengths. These include established executive and governance oversight, continued expansion of multi-factor authentication, proactive vulnerability management, resilient and immutable backup arrangements, cyber incident response processes and 24-hour external monitoring through both Third party supplied Managed Detection and Response (MDR) and the NHS national Cyber Security Operations Centre (CSOC). Both monitoring services have detected and stopped security incidents affecting NEAS during the previous six months.

A further significant source of assurance is provided by the Emergency Preparedness, Resilience and Response team (EPRR). Cyber security controls are intended to prevent, detect and contain incidents, but EPRR arrangements provide organisational assurance that critical services can continue when preventative or technical controls are unsuccessful. Reciprocal representation is now in place, with IM&T represented at the Emergency Preparedness, Resilience and Response Group (EPRRG) and EPRR represented at the IT & Security Working Group (ITSG).

The current position is therefore positive. However, it should not be interpreted as indicating that all cyber risks have been addressed or that all systems and services demonstrate the same level of cyber maturity. No material gap has been identified against the Trust's current DSPT status, but substantial future activity will be required to meet progressively increasing DSPT and CAF expectations.

From September 2026, NHS England intends to introduce new and updated directive cyber policies covering matters including multi-factor authentication, high-severity alerts and endpoint detection. The DSPT will also be updated to incorporate CAF 4.0, with requirements expected to tighten each year through to 2030. NHS England has expressly stated that incremental progress and investment are expected year on year.

These changes will have significant implications for the Trust. Some can be delivered through policy, governance and process improvements, but others will require substantial redesign of existing infrastructure, systems and operating arrangements. Delivery will require investment in technology, sufficient specialist capacity, stronger architectural and assurance functions and support for the implementation of recommendations arising from the ongoing IM&T structural review.

NEAS currently has substantial assurance but with continuous improvement and strategic investment required to maintain that assurance.