Hertfordshire Partnership University
NHS Foundation Trust

20 November 2025

Information Rights & Compliance Team
99 Waverley Road
St Albans
Hertfordshire
AL3 5TL

Tel: 01727 804227
Email: Hpft.foi@nhs.net

Our Ref: FOI/05910

Thank you for your request concerning how our Trust organises and oversees cybersecurity governance and organisational learning.

Your request has been considered and processed in accordance with the requirements of the Freedom of Information (FOI) Act 2000.

Please provide information for the period 1 January 2018 – 31 December 2024 (inclusive) or the most recent complete year available.

1. **Governance framework — The framework used for cybersecurity governance (e.g. NCSC CAF, DSPT, ISO 27001) and the year of its latest board approval.**
   The Trust uses the Cyber Assessment Framework (CAF) Aligned Data Security and Protection Toolkit(DSPT) for cybersecurity governance and provides annual self-assessments against this framework to NHS England. The last submission was made in June 2025 for the 2024/25 fiscal year.

2. **Board review frequency — How often the board or an executive committee formally reviews cyber resilience or cybersecurity governance (e.g. annually, quarterly, ad hoc).**
   The Trust's Information Management and Governance Subcommittee (IMGS) is responsible for cybersecurity and receives quarterly cybersecurity reports. IMGS also oversees cybersecurity risks.
   Cyber resilience arrangements are also tested annually through Trust-wide (or sometimes multiorganizational) cyber security exercises annually via the Trust's Emergency Preparedness, Resilience and Response Team.

3. **Most recent review — The title and month/year of the latest board or committee paper or report relating to cyber resilience (no internal findings required).**
   The last cybersecurity report (Quarter 2 2025/26) was presented to the IMGS on 7th November ,2025.

4. **Reporting line — The current reporting structure for cybersecurity governance (e.g. CISO → CIO → Board).**
   IMGS Audit Committee Trust Board.
   Please note that IMGS also reports to the Trust's Executive Team after each meeting. Please also note that prior to November 2025, IMGS reported to the Integrated Governance Committee.

5. **External assurance — Whether the Trust has undergone external assurance such as CAF self-assessment, DSPT validation, independent audit, or security testing (e.g. penetration test / red-team). If so, please indicate only the type and frequency, not the scope or results.**

The Trust's CAF Aligned DSPT toolkit submission is audited independently by the Trust's internal auditors annually prior to submission. The Trust also carries out annual penetration testing and simulated phishing exercises. In September 2024, the Trust's also undertook a one-off voluntary audit of its information and cyber security arrangement by the Information Commissioner's Office.

6. **Concurrent improvement programmes — Approximate number of cybersecurity-related improvement programmes or initiatives active concurrently in a typical year (2018–2024) and trend (increasing/decreasing/stable).**
The information you are requesting relating to our cybersecurity-related improvement programmes or initiatives if answered could be used to compromise the security of the organisation. It would make the organisation vulnerable to a crime such as hacking and this could lead to a theft of information or a denial of service to IT systems therefore we have applied S31(1)(a) – Law Enforcement (1)

Information is exempt if its disclosure under this Act world or would be likely to prejudice (a) the prevention or detection of crime.

Section 31 is subject to a test of prejudice. Please see below for our considered reasons for and against disclosure:

Reason in favour of disclosure
We acknowledge the public interest in openness and transparency and recognise that releasing this information would provide the public with assurance that we are protecting their information and our technologies.

Reason against disclosure
Disclosure of the our system would make the Trust vulnerable to cybercrime as it outlines the Trust's security position which could be used as a starting point to attack network infrastructure and/or information systems. We have reached the view that on balance, the public interest is better serviced by withholding this information under the section 31(1) exemption.

7. **Internal coordination — Whether a steering group, programme office, or committee coordinates concurrent cybersecurity initiatives within the Trust, and its reporting level (executive/board).**
This is coordinated by the IMGS. Please see question 4 for the reporting lines.

8. **Cross-Trust coordination — Whether the Trust participates in structured coordination or information-sharing mechanisms with other NHS Trusts or regional bodies on cyber-resilience governance (e.g. ICS cyber networks), and at what level (regional/national).**
The Trust is member of the national NHS Cyber Associates Network, receives threat alerts from the national cybersecurity team and weekly Cyber Alert Bulletins from NHS England.
The Trust's cybersecurity services are provided by a shared service which also provides the same service to three other organisations.

9. **Board learning — Whether board-level training sessions or workshops on cyber resilience have been held since 2018, and in which years.**
There has been no board-level training sessions or workshops specifically on cyber resilience. However, the Audit Committee and the Executive Team have done deep dive sessions on this topic.

Should you require further clarification, please do not hesitate to contact me.

Please find enclosed an information sheet regarding copyright protection and the Trust's complaints procedure in the event that you are not satisfied with the response.

Yours sincerely

D. Anthony

Deborah Anthony

Information Rights Officer

Enc: Copyright Protection and Complaints Procedure Information Leaflet.

If you would like to complete a short survey in relation to your Freedom of Information request please click here.