Hertfordshire Partnership University
NHS Foundation Trust

26 January 2023

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

Tel: 01727 804954
Email: Hpft.foi@nhs.net

Our Ref: FOI/04569

Thank you for your request concerning Cybersecurity.

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

1. **What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?**
2. **What is the classification of your policy regarding breach response?**
3. **Of the devices running Windows operating systems, what is the number and percentage of devices running Windows 11, Windows 10, Windows 7, Windows XP?**
4. **What are the top 20 cyber security risks in your Trust, and how are they managed?**
5. **Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.**
6. **What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows , Windows XP)?**
7. **What is your current status on unpatched Operating Systems?**
8. **Of the devices running Windows Servers operating systems, what is the number and percentage of devices running Windows 2000, Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019, Windows 2022?**

The information you are requesting in questions 1 to 8 are relating to our cyber security and 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.

S31 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 number of cyber-attacks and the use of certain operating systems / platforms would make the Trust vulnerable to cyber-crime 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.

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience?

We do not hold this information[1]. This is managed under our Service Level Agreement (SLA) with another IT Service Provider.

If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?

We have applied S31 to this question[2]. Please see justification given under question 8.

10. Does your Trust hold a cyber insurance policy? If so:
- **a) What is the name of the provider;**
- **b) How much does the service cost; and**
- **c) By how much has the price of the service increased year-to-year over the last three years?**

We have applied S31 to this question[2]. Please see justification given under question 8.

11. When did the current Board last receive a briefing on cybersecurity threats within healthcare, and when did they last participate in cyber security training? How frequently, if at all, do these briefings and trainings occur, and are they carried out by cyber security technology professionals?

We have applied S31 to this question[2]. Please see justification given under question 8.

12. Has your NHS Trust completed a Connection Agreement to use the Health and Social Care Network (HSCN)? If so, did you pass, and is there a copy of the code of connection?

We do not hold this information[1]. Our core HSCN connections are managed by another IT Service provider.

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?

No.

14. How many open vacancies for cyber security positions are there within your Trust, and is their hour capacity affected by a shortage of qualified applicants?

We do not hold this information[1]. This is managed under our Service Level Agreement (SLA) with another IT Service Provider.

15. Are there mandatory minimum training requirements for those transferred internally to work in
cybersecurity within your Trust, and if so, how often is the training updated and revised to reflect the evolving nature of the industry?

We do not hold this information[1]. This is managed under our Service Level Agreement (SLA) with another IT Service Provider.

---

[1] Section 1(1) Any person making a request for information to a public authority is entitled
(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
(b) if that is the case, to have that information communicated to him.

[2] Section 31 - 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

16. **How much money is spent by your Trust per year on public relations related to cyber attacks? What percentage of your overall budget does this amount to?**

We have applied S31 to this question[2]. Please see justification given under question 8.

17. **Does your Trust have a Chief Information Risk Officer? If so, who do they report to?**

Yes we do, they report to the Board.

18. **When was the last time your Trust underwent a security audit? At what frequency do these audits occur?**

We regularly audit our security. We have applied S31 to providing any more details regarding our security audit. Please see justification given under question 8.

19. **What is your strategy to ensure security in cloud computing?**

We have applied S31 to this question[2]. Please see justification given under question 8.

20. **Do you purchase additional / enhanced support from a Supplier for end-of-life software (Operating Systems / Applications)? If so, what are the associated costs per year per Operating System / Application, and the total spend for enhanced support?**

This is managed under SLA with another IT Service Provider.

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

Sue Smith

Sue Smith
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 scan the QR code below or click here.