University Hospitals Bristol and Weston NHS Foundation Trust

Freedom of Information Request **Ref: 23-038**

10 February 2023

By Email

Dear Sir/Madam

Thank you for your request for information under the Freedom of Information Act 2000. The Trust's response is as follows:

- We can confirm that we do hold the information you are requesting

University Hospital Bristol and Weston NHS Foundation Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31

S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

Factors in favour of confirming or denying the information is held

The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the Trust's digital infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's digital security.

Factors in favour of neither confirming nor denying the information is held

Cyber-attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks and, since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

Balancing the public interest factors

The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extend the Trust is able to detect and deal with digital security attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's digital systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's digital systems.

1. What was the total number of cyber attack incidents that have been recorded in your trust in the past 24 months?
0

2. What is the classification of your policy regarding breach response?
Classified

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?
Please refer to our section 31 exemption statement above

4. What are the top 20 cyber security risks in your Trust, and how are they managed?
Please refer to our section 31 exemption statement above

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed.
Internal Risk Frameowrk

6. What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows, Windows XP)?
Please refer to our section 31 exemption statement above

7. What is your current status on unpatched Operating Systems?
Please refer to our section 31 exemption statement above

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?
Please refer to our section 31 exemption statement above

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation?
Please refer to our section 31 exemption statement above

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?
Please refer to our section 31 exemption statement above

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?
Within the last month

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?
Yes. Code of connection is available from NHS England (formerly NHS Digitial)

13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?
Please refer to our section 31 exemption statement above

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?
None

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?
Please refer to our section 31 exemption statement above

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?
0

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?
Yes, Director of Finance and Information

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?
Please refer to our section 31 exemption statement above

19. What is your strategy to ensure security in cloud computing?
Please refer to our section 31 exemption statement above

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?
Please refer to our section 31 exemption statement above

This concludes our response. We trust that you find this helpful, but please do not hesitate to contact us directly if we can be of any further assistance.

If, after that, you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to:

Data Protection Officer
University Hospitals Bristol and Weston NHS Foundation Trust
Trust Headquarters
Marlborough Street
Bristol
BS1 3NU

Please remember to quote the reference number above in any future communications.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

<u>Publication</u>

Please note that this letter and the information included/attached will be published on our website as part of the Trust's Freedom of Information Publication Log. This is because information disclosed in accordance with the Freedom of Information Act is disclosed to the public, not just to the individual making the request. We will remove any personal information (such as your name, email and so on) from any information we make public to protect your personal information.

To view the Freedom of Information Act in full please click here.

Yours sincerely

Freedom of Information Team
University Hospitals Bristol and Weston NHS Foundation Trust