Freedom of Information Act 2000 - Request Reference FoI/23/028
Digital Infrastructure

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

   Cardiff and Vale University Health Board (the UHB) is withholding this information, relying on Section 31(1)(a) of the Freedom of Information Act 2000 (prevention and detection of crime). Specifically, the UHB believes that disclosing details regarding its ICT infrastructure, or support of that infrastructure, would be likely to prejudice the prevention of crime, particularly cyber-crime. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

   Public Interest Test:

   In favour of disclosure: The UHB recognises there is a public interest in transparency and in public authorities demonstrating that their systems effectively protect personal data.

   Against disclosure: There is a very strong public interest in protecting the extremely sensitive data held by the UHB. Cyber Security and the associated Cyber-Risk / Cyber-Attacks represent a rapidly evolving arena that becomes more complex and dangerous with time. Releasing details of the UHB's ICT infrastructure into the public domain significantly reduces its capacity to manage this threat to the stated public interest by exposing potential vulnerabilities.

   Decision: The UHB considers that the public interest in withholding the information is significantly greater than any interest there may be in disclosing it and potentially exposing sensitive personal data to an increased level of risk. The UHB strongly believes that posing additional unnecessary risk to the UHB, and consequently patient care and safety, would be viewed as an unacceptable risk by the public. Whilst the UHB acknowledges a public interest in providing assurances of effective protection of personal data, it believes the most effective means of increasing public confidence in data protection is to successfully protect the data itself. The UHB considers its responsibility to protect the personal data of patients and staff to be of the highest importance. It was therefore decided that it was not in the public's interest to disclose this information.

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

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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?**

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

4. **What are the top 20 cyber security risks in your Trust, and how are they managed?**

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

6. **What is your Patch Management Cycle and how is it implemented on old Operating systems (e.g., for Windows, Windows XP)?**

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

7. **What is your current status on unpatched Operating Systems?**

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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 UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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?**

   The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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;**
    c. **By how much has the price of the service increased year-to-year over the last three years?**

    After considering your request, Cardiff and Vale University Health Board (the UHB) considers this information to be exempt from disclosure under the Freedom of Information Act 2000 (Section 43) Commercial Interests. This section of the Act sets out an exemption from the right to know if:

- the information requested is a trade secret, or
- release of the information is likely to prejudice the commercial interests of any person. (A person may be an individual, a company, the public authority itself or any other legal entity).

This exemption was considered by the UHB when deciding whether to disclose information because it considered that in doing so there could be a significant risk in prejudicing the commercial interests of both Cardiff University and the UHB. As this is a qualified exemption, the UHB is required to complete a public interest test in deciding whether it is in the public's interest to withhold or disclose the information.

In favour of disclosure: There is a public interest in transparency and in the accountability of spending of public funds. Furthermore, it is in the public's interest that public funds be used effectively and that public sector bodies obtain the best value for money when contracting for the provision of services.

Against disclosure: It has been established that releasing the information sought under the Freedom of Information Act, to which the UHB is subject, will give an unfair advantage to the supplier's competitors. There is a risk of disclosure prejudicing the commercial interests of the UHB by affecting its bargaining position with suppliers. This in turn could lead to less effective use of public funds in future. The UHB believes that there is wider established public interest in suppliers not being prejudiced merely because they have contracted with a public sector body (as upheld in ICO decision notice FS50473543 ICO v Royal Marsden Hospital Trust).

Decision: The UHB considers that the public interest in withholding the information is greater than the interests in disclosing it and thereby giving unfair commercial advantage to competitors of the supplier to which this information concerns. The UHB believes that disclosure of information in a manner which fails to protect the interests and relationships arising in a commercial context could have the effect of discouraging companies from dealing with the Health Board because of fears that the disclosure of information could damage them commercially. In turn this could then jeopardise the Health Board's ability to compete fairly and pursue its function to bring forward development in the area and obtain value for money. It was therefore decided that it was not in the public's interest to disclose this information.

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?

Cyber Awareness training provided to the Board at a Development Session on 25th August 2022. Briefing shared with Board members since then. Standing item at the digital sub-committee of the Board.

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?

The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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?

1

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?

The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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?

The UHB does not hold this information.

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

No.

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

The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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

The UHB believes that Section 31(1)(a) of the Freedom of Information Act 2000 applies here, please see the exemption set out in question 1.

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?

The UHB believes that Section 43 (Commercial Interests) applies here. Please see the exemption set out in question 10.