The Dudley Group
NHS Foundation Trust

Freedom of Information request 017594

10/2/23

I am writing to you to request the following information about your NHS Trust under section 1(1) of the Freedom of Information Act 2000:

Please note for questions 1, 2, 3, 4, 6, 7, 8, 9, 10, 12, 19 & 20 an exemption has been applied :-
The Trust is required to balance whether the information requested is in the public interest (the public as a whole) and if the release of such information would have the potential to cause any harm should that information get into the wrong hands.
It Is imperative that the Trust is cyber resilient, cyber-attacks against infrastructure have the potential to inflict significant, real-life disruption and prevent access to critical services that are vital to the functioning of Trust systems. The Trust considers this information to be sensitive information and are therefore holding this information under section 31 (1) of the Freedom of Information Act. Information - is exempt if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime

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

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

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? - exemption

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

5. Do you continue to use the Unified Cyber Risk Framework, is so how many risks are still identified/managed. - Not currently

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

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

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? - exemption

9. Has your Trust signed up to and implemented the NHS Secure Boundary managed service to strengthen cyber resilience? - Yes
If so, how many cyber security threats has the NHS Secure Boundary detected within your NHS Trust since its implementation? - exemption

10. Does your Trust hold a cyber insurance policy? If so: - exemption
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?

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? - Monthly Cyber Reports to Board. All staff complete annual mandatory training which includes Cyber Security

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? - exemption

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? - Zero

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? - Staff employed or transferred into the IT/Cyber teams would be assessed on existing skills and experiences prior to starting. Annual mandatory training includes cyber security for all staff – content is reviewed annually or by exception. Specialist training for the Cyber team is determine via appraisals and emerging technologies and threats

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? - None to date

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to? - Yes the Trust has a Senior Information Risk Officer in place reporting directly to the Chief Executive

18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur? **-** December 2022 – annual audit

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

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? - exemption

The Trust has many requests for information on IT systems, to see previous response please go to the Freedom of Information request disclosure log on the Trust website Freedom of information - The Dudley Group NHS Foundation Trust (dgft.nhs.uk) and in the 'search' box type in IT systems