Royal Devon University Healthcare NHS Foundation Trust

Cyber Security

Reference Number: RDF1210-23
Date of Response: 17/02/2023

Further to your Freedom of Information Act request, please find the Trust's response(s) below:

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?
The Board receive annual Data Security and Protection Training, that includes a cyber security element and is an online course undertaken at different times by each board member so we are unable to provide a date.
They also receive specific Board level Information Governance and Security training every two years which includes cyber security, this was last undertaken in 2021. In addition, there is Board attendance at the annual DSPT data security incident exercise. Briefings may also be provided to Board members in line with any current threats of incidents.

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 information that you have requested is exempt under Section 21 of the Freedom of Information Act because it is reasonably accessible to you. The information you requested can be accessed via the via the following link:-

: https://crm.digital.nhs.uk/hscnconnectionagreementsearch/

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?
There are no currently published vacancies for cyber security positions.

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?.
Security job descriptions feature essential and desirable experience. A training needs analysis (TNA) of staff with specialist training is maintained to ensure relevant staff are appropriately trained.

17. Does your Trust have a Chief Information Risk Officer? If so, who do they report to?. The Trust has a Senior Information Risk Owner (SIRO) who is a Board member and reports to the CEO.

19. What is your strategy to ensure security in cloud computing?.: Purchases of IT equipment and services are to be reviewed by Digital Services so security considerations are taken into account.

The Trust is unable to provide a response to the following questions. We do not confirm or deny if information is held where it relates to cyber security and could impact on the security of our systems and information held within them in line with Section 31 of the Freedom of Information Act.

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?
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?.
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?.
13. Have there been any incidents of staff members or personnel within your Trust being let go due to issues surrounding cyber security governance?.
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?.
18. When was the last time your Trust underwent a security audit? At what frequency do these audits occur?.
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?.

Section 31(3) of the Freedom of Information Act 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. Section 31(3) is subject to a public interest test for determining whether the public interest lies in confirming if the information is held or not.

Factors in favour of confirming or denying the information is held.

The Trust considers that to release the requested information would reveal details that could assist in a cyber-attack. However the Trust recognises that answering the request would promote openness and transparency with regards to the Trust’s IT security.

Cyber-attacks which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018, 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 providing the requested information would also provide information about the Trust's information 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. Releasing the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

As an Operator of Essential Services:
(https://www.legislation.gov.uk/uksi/2018/506/schedule/2/paragraph/8), the Trust must comply with The Network and Information Systems Regulations 2018. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in section 10 (https://www.legislation.gov.uk/uksi/2018/506/regulation/10) of the Network and Information Systems Regulations 2018.

The prejudice in complying with Section 31(3) of FOIA is real and significant and would allow valuable insight into the perceived strengths and weaknesses of the Trust's IT infrastructure and information systems.