University Hospitals Bristol and Weston NHS Foundation Trust

Freedom of Information Request **Ref: 21-439**

21 September 2021

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 hold some the information you are requesting

1. What is your annual IT Budget for 2021, 2022 & 2023?
2021 - £10,890,857
2022 - £12,644,404
2023 £ not yet known

2. Storage:
a. What storage vendor(s) and models do you currently use?
TinTri, EMC Isilon, VPLEX, Unity

b. What is the capacity of the storage data in TB & How much of this is utilised?
2.1PB , 1.3PB used

c. What were the installation dates of the above storage vendor(s)? (Month/Year)
It varies

d. When is your planned (or estimated) storage refresh date? (Month/Year)?
September 2021, Dec 2021, September 2022

e. Do you have any extended warranties, if so, with which supplier?
TinTri and Isilon and VPEX Unity, Exagrid

f. What is your estimated budget for the storage refresh?
£600,000

3. Server/Compute:
a. What server vendor(s) and models do you currently use?
Dell

b. What were the installation dates of the above server vendor(s)? (Month/Year)
It varies

c. When is your planned (or estimated) server refresh date? (Month/Year)
November annually

d. What is your estimated budget for the server refresh?
£200,000

e. Do you have any extended warranties, if so, with which supplier?
Dell

f. Which operating systems are used?
Windows and Linux of multiple versions and distros

4. Backup, DR and BC:
a. What device/system do you use for your daily backups (e.g tape or disk)
Disk

b. What backup software do you use?
Primarily Veeam but a number of departments utilise their own software

c. How much data do you backup, in TB?
330

d. Do you use a third party to provide a Business Continuity service (e.g. office workplace recovery or infrastructure ship-to-site solutions)?
No

e. Does your current recovery solution meet your stakeholder's RTO/RPO expectations?
Yes

f. Do you already backup into the cloud?
No

g. Do you have a documented disaster recovery & business continuity plan in place?
Yes

5. Number of Physical servers?
35

6. Number of virtualised servers? & Which Virtualisation platform do you use?

721- VMware

7. Security:
a. What security solutions are being utilised?
b. Do you have a SIEM?
c. Do you have a SOC? If so, is it in house or outsourced?
d. Is it 24/7?
e. Name and role for IT Manager(s) / Officer(s) primarily responsible for cybersecurity
f. Names of all cyber security vendor(s) you us
g. Cost, duration and end date for the above contract(s)/license(s)
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.

8. How far are you in your cloud strategy?
A. Not considering Cloud for the foreseeable future
B. Interested in Cloud, but have not started looking into it ✓
C. Research Stage
D. Meeting with Suppliers
E. Consultancy
F. Started to integrate
G. Fully integrated

9. Which public cloud provider do you use?
Azure

10. Which IT services do you outsource? When do the contracts end?
None

11. Please also name all of the IT re-sellers that you work with and buy from, as well as the frameworks utilised.
CDW, Dell, WPDM, MTI, NG-IT, ManageEngine, Globalsign, Pheonix

12. Are you actively moving any applications/infrastructure into a cloud environment? If so who is responsible for this?
No

13. Do you normally purchase equipment and services as a capital investment (Cap-Ex) or ongoing operational charges (Opex)?
Cap-Ex if possible

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:

Director of Corporate Governance
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

Publication

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