

Freedom of Information Request

Ref: 21-475

7 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 do hold the information you are requesting**
- 1. **In the past three years has your organisation:**
 - a. **Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?)**
 - i. **If yes, how many?**
 - b. **Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)**
 - c. **Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.)**
 - d. **Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?**
 - i. **If yes was the decryption successful, with all files recovered?**
 - e. **Used a free decryption key or tool (e.g. from <https://www.nomoreransom.org/>)?**
 - i. **If yes was the decryption successful, with all files recovered?**
 - f. **Had a formal policy on ransomware payment?**
 - i. **If yes please provide, or link, to all versions relevant to the 3 year period.**
 - g. **Held meetings where policy on paying ransomware was discussed?**

h. Paid consultancy fees for malware, ransomware, or system intrusion investigation

i. If yes at what cost in each year?

i. Used existing support contracts for malware, ransomware, or system intrusion investigation?

j. Requested central government support for malware, ransomware, or system intrusion investigation?

k. Paid for data recovery services?

i. If yes at what cost in each year?

l. Used existing contracts for data recovery services?

m. Replaced IT infrastructure such as servers that have been compromised by malware?

i. If yes at what cost in each year?

n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?

i. If yes at what cost in each year?

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 extent 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.

o. Lost data due to portable electronic devices being mislaid, lost or destroyed?

Yes

i. If yes how many incidents in each year?

2019 - 1

2021 - 3

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365?

Yes

a. If yes is this system's data independently backed up, separately from that

platform's own tools?

No

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

- a. Mobile devices such as phones and tablet computers - No
- b. Desktop and laptop computers - No
- c. Virtual desktops - No
- d. Servers on premise - Yes
- e. Co-located or hosted servers - Yes
- f. Cloud hosted servers - No
- g. Virtual machines - Yes
- h. Data in SaaS applications - Some
- i. ERP / finance system - Yes
- j. We do not use any offsite back-up systems - Not applicable

4. Are the services in question 3 backed up by a single system or are multiple systems used?

Multiple Systems are used

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

No

6. How many Software as a Services (SaaS) applications are in place within your organisation?

10

a. How many have been adopted since January 2020?

2

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