The Walton Centre NHS
NHS Foundation Trust
Excellence in Neuroscience

Date: Wednesday, 01st September 2021
Our Ref: MB/SS FOI 4873

Sid Watkins Building
Lower Lane
Fazakerley
Liverpool L9 7BB
Tel: 01515253611
Fax: 01515295500
Direct Line: 01515563038

Re: Freedom of Information Request FOI 4873

We are writing in response to your request submitted under the Freedom of Information Act, received in this office on 01st September 2021.
Your request was as follows:

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?

The Walton Centre NHS Foundation Trust has had 1 cyber-attack in the past 3 years.

b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)

I confirm that The Walton Centre NHS Foundation Trust holds the information you have requested. However, I am unable to provide you with that information as I consider that the following exemptions apply to it:

Section 31 (1a) - The prevention or detection of crime
This information is exempt from disclosure under Section 31 (1a) of the Freedom of Information Act 2000 (FOIA). We consider that if the data you have requested were to be combined with other information which may be available in the public domain, there would likely to be an increased risk of a cyber-security attack upon the Trust. As part of the Critical National Infrastructure for the NHS, the Trust has a duty to protect the integrity of our systems. The disclosure of the information requested could expose weaknesses in our systems and lead to breaches, making the UK or its citizens, in this case our patients, more vulnerable to security threat.

Public Interest Test
To use this exception we are required to undertake a public interest test. The matters which were considered in applying the public interest test are as follows:

Factors in favour of disclosure:
• Disclosure of the data supports the general public interest in the transparency, accountability and general understanding of the delivery of public services.

Factors in favour of withholding:
• Breaches in Trust security and is therefore a reasonable threat to the confidential patient data held on our systems.

- Temporary or long term lack of availability of IT systems
- Corruption/loss of patient data which would prevent or interrupt provision of patient care.

There is a strong public interest in protecting the confidentiality of patient data and of ensuring that healthcare services can be provided to the public without increasing the possibility of attack by hackers or malware, or of putting personal or other information held on these systems at risk of corruption or subject to illegal access. For these reasons, the Trust has decided that it is in the public interest to withhold this information at this time.

This response therefore acts as a refusal notice under section 17 of the FOIA.

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.)

As above.

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?

As above.

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?

As above.

f. Had a formal policy on ransomware payment?

i. If yes please provide, or link, to all versions relevant to the 3 year period.

As above.

g. Held meetings where policy on paying ransomware was discussed?

As above.

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

i. If yes at what cost in each year?

As above.

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

As above.

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

As above.

k. Paid for data recovery services?

i. If yes at what cost in each year?

As above.

l. Used existing contracts for data recovery services?

As above.

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

i. If yes at what cost in each year?

As above.

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?

As above.

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

i. If yes how many incidents in each year?

As above.

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

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

As above.

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

b. Desktop and laptop computers

c. Virtual desktops

d. Servers on premise

e. Co-located or hosted servers

f. Cloud hosted servers

g. Virtual machines

h. Data in SaaS applications

i. ERP / finance system

j. We do not use any offsite back-up systems

As above.

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

As above.

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

As above.

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

a. How many have been adopted since January 2020?

As above.

Please see our response above in blue.

Re-Use of Public Sector Information

All information supplied by the Trust in answering a request for information (RFI) under the Freedom of Information Act 2000 will be subject to the terms of the Re-use of Public Sector Information Regulations 2005, Statutory Instrument 2005 No. 1515 which came into effect on 1st July 2005.

Under the terms of the Regulations, the Trust will licence the re-use of any or all information supplied if being used in a form and for the purpose other than which it was originally supplied. This license for re-use will be in line with the requirements of the Regulations and the licensing terms and fees as laid down by the Office of Public Sector Information (OPSI). Most licenses will be free; however the Trust reserves the right, in certain circumstances, to charge a fee for the re-use of some information which it deems to be of commercial value.

Further information can be found at www.opsi.gov.uk where a sample license terms and fees can be found with guidance on copyright and publishing notes and a Guide to Best Practice and regulated advice and case studies, at www.opsi.gov.uk/advice/psi-regulations/index.htm

If 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 the Freedom of Information Office at the address above.

Please remember to quote the reference number, FOI 4873 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 Commissioners Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely

Mike Burns

Mr. Mike Burns, Executive Lead for Freedom of Information