Date: Wednesday, 01st December 2021
Our Ref: MB/SS FOI 4969

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

Re: Freedom of Information Request FOI 4969

We are writing in response to your request submitted under the Freedom of Information Act, received in this office on 30th November 2021.
Your request was as follows:

1. Do you have a formal IT security strategy? (Please provide a link to the strategy)

A) Yes

B) No

I confirm that The Walton Centre NHS Foundation Trust (WCFT) 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 21 - Information already reasonably accessible to you
This information is exempt from disclosure under Section 21 of the Freedom of Information Act 2000 (FOIA), as it is already reasonably accessible to you. The information you have requested is published on The Walton Centre NHS Foundation Trust (WCFT) website, please use the following link:

- https://www.thewaltoncentre.nhs.uk/Downloads/Reports-and-Publications/Strategies/Digital%20Strategy%202020.pdf

This exemption is not subject to the public interest test. This response therefore acts as a refusal notice under section 17 of the FOIA.

2. Does this strategy specifically address the monitoring of network attached device configurations to identify any malicious or non-malicious change to the device configuration?

A) Yes

B) No

C) Don't know

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.

3. If yes to Question 2, how do you manage this identification process - is it:

A) Totally automated - all configuration changes are identified and flagged without manual intervention.

B) Semi-automated - it's a mixture of manual processes and tools that help track and identify configuration changes.

C) Mainly manual - most elements of the identification of configuration changes are manual.

See response for question 2.

4. Have you ever encountered a situation where user services have been disrupted due to an accidental/non malicious change that had been made to a device configuration?

A) Yes

B) No

C) Don't know

See response for question 2.

5. If a piece of malware was maliciously uploaded to a device on your network, how quickly do you think it would be identified and isolated?

A) Immediately

B) Within days

C) Within weeks

D) Not sure

See response for question 2.

6. How many devices do you have attached to your network that require monitoring?

A) Physical Servers: record number

B) PC's & Notebooks: record number

See response for question 2.

7. Have you ever discovered devices attached to the network that you weren't previously aware of?

A) Yes

B) No

See response for question 2.

If yes, how do you manage this identification process - is it:

A) Totally automated - all device configuration changes are identified and flagged without manual intervention.

B) Semi-automated - it's a mixture of manual processes and tools that help track and identify unplanned device configuration changes.

C) Mainly manual - most elements of the identification of unexpected device configuration changes are manual.

See response for question 2.

8. How many physical devices (IP's) do you have attached to your network that require monitoring for configuration vulnerabilities?

Record Number:

See response for question 2.

9. Have you suffered any external security attacks that have used malware on a network attached device to help breach your security measures?

A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

See response for question 2.

10. Have you ever experienced service disruption to users due to an accidental, non-malicious change being made to device configurations?

A) Never

B) Not in the last 1-12 months

C) Not in the last 12-36 months

See response for question 2.

11. When a scheduled audit takes place for the likes of PSN or Cyber Essentials, how likely are you to get significant numbers of audit fails relating to the status of the IT infrastructure?

A) Never

B) Occasionally

C) Frequently

D) Always

See response for question 2.

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 4969 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