The Walton Centre NHS
NHS Foundation Trust
Excellence in Neuroscience

Date: Thursday, 11th May 2023
Our Ref: MB/CM FOI 5687

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

Re: Freedom of Information Request FOI 5687

We are writing in response to your request submitted under the Freedom of Information Act, received in this office on 13th April 2023.
Your request was as follows:

What is your primary inventory method for tracking each device type connected to the network?

IT devices (i.e. pc, laptop)

•□CMDB

•□Manual spreadsheet

•□Automated device detection

•□Other

•□None

IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)

•□CMDB

•□Manual spreadsheet

•□Automated device detection

•□Other

•□None

Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)

•□CMDB

•□Manual spreadsheet

•□Automated device detection

•□Other

•□None

OT and building automation

(i.e. heating and cooling, routers, switches)

•□CMDB

•□Manual spreadsheet

•□Automated device detection

•□Other

•□None

IT Devices - Automated device detection
IoT - None - all fixed/static items
Connected Medical Devices - Manual spreadsheet
OT and building automation - None - all fixed/static items

How often is the information on those systems updated?

IT devices (i.e. pc, laptop)

•□As changes occur (real-time)

•□Daily

•□Weekly

•□Monthly

•□Quarterly

•□Annually

•□Never

•□I don't know

IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)

•□As changes occur (real-time)

•□Daily

•□Weekly

•□Monthly

•□Quarterly

•□Annually

•□Never

•□I don't know

Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)

•□As changes occur (real-time)

•□Daily

•□Weekly

•□Monthly

•□Quarterly

•□Annually

•□Never

•□I don't know

OT and building automation

(i.e. heating and cooling, routers, switches)

•□As changes occur (real-time)

•□Daily

•□Weekly

•□Monthly

•□Quarterly

•□Annually

•□Never

•□I don't know

IT devices - As changes occur (real-time)
IoT - N/A
Connected Medical devices - As changes occur (real-time)
OT and building automation - As changes occur (real-time) BMS is a "Live" system and updates automatically

Was cybersecurity discussed by the Trust Board within the last 12 months? Y/N

What were the priorities discussed? (select all that apply)

•□Keeping up with threat intelligence

•□Medical device security

•□Allocating cybersecurity spending

•□Visibility of all assets connected to the network

•□Staffing/recruitment

•□Compliance with checking cybersecurity regulations/frameworks

•□Securing the supply chain

•□Dealing with ransomware

•□IoT / OT Security

•□Connected Chinese or Russian made devices

•□Other:

How often is cybersecurity discussed by the board

- Every 3 months
- every 6 months
- Every 12 months
- Ad hoc
- Never

Was cybersecurity discussed by the Trust Board within the last 12 months? - Yes
How often is cybersecurity discussed by the board? - Several times a year and adhoc depending on the situation.

What were the priorities discussed?

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.

•□Is medical device security a specific project on your roadmap for the next 12 months?

•□Are you able to respond to high severity NHS cyber alerts within the stated 48 hour timeline and patch within two weeks from disclosure?

•□ What are the main challenges in meeting NHS Cyber Alert timelines?

•□What is your process for mapping individual NHS Cyber Alerts to every device on your network?

•□Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?

•□Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?

•□Are you able to attract and retain sufficient numbers of IT staff to fill available roles?

•□Do you feel you have sufficient IT staff to meet the demands placed upon you?

•□Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?

•□In the past year, has a cyberattack originated from a 3rd party vendor with access to your network (supply chain attack)? If so, what service did the 3rd party provide (not company names)?

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.

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 5687 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 by:

Post: Information Commissioners Office, Wycliffe House, Water Lane, Wilmslow, CHeshire, SK9 5AF.

Online: https://ico.org.uk/make-a-complaint/foi-and-eir-complaints/

Telephone: 0303 123 1113

Yours sincerely

Mike Burns
Mr. Mike Burns, Executive Lead for Freedom of Information