University Hospitals
Bristol and Weston
NHS Foundation Trust

Freedom of Information Request   Ref: 23-264

16 May 2023

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 of the information you are requesting

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
Automated device detection

IoT (i.e smart Tvs, smart watches, assistants like Alexa, Siri)
• CMDB
• Manual spreadsheet
• Automated device detection
• Other
• None
Other

Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
• CMDB
• Manual spreadsheet
• Automated device detection
• Other
• None
We use a system called Medusa for tracking connected medical devices and this is updated as changes occur (real time).

OT and building automation
(i.e. heating and cooling, routers, switches)

- **CMDB**
- **Manual spreadsheet**
- **Automated device detection**
- **Other**
- **None**

Not applicable - we do not track these devices.

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**

Weekly

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**

Annually

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**

We use a system called Medusa for tracking connected medical devices and this is updated as changes occur (real time).

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
Not applicable - we do not track these devices.

Was cybersecurity discussed by the Trust Board within the last 12 months? Y/N Yes
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:
We are withholding this information under section 31.
The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems again criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations,

How often is cybersecurity discussed by the board
• Every 3 months
• every 6 months
• Every 12 months
• Ad hoc Ad hoc – cyber security is also discussed at the Finance and Digital Committee – a committee of the Trust board that has oversight of digital issues.
• Never
• Is medical device security a specific project on your roadmap for the next 12 months?
Medical device security is always a high priority for the trust and will continue to be monitored in 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?
We are withholding this information under section 31.
The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems again criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations,

• What are the main challenges in meeting NHS Cyber Alert timelines?
We are withholding this information under section 31.
The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems again criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations,

• What is your process for mapping individual NHS Cyber Alerts to every device on your network?
We are withholding this information under section 31.
The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems again criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations,

• Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?
Not applicable.

• Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?
Equipment which becomes unsupported is identified as part of the planning process. The Trust uses a risk-based approach to prioritise the replacement of medical equipment to ensure that resources are deployed to the highest priority.

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

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

• Approximately how long does it take for the Trust to assess on Data Security and

Protection Toolkit (DSPT)? What takes the most time?
The Data Security and Protection Toolkit is assessed annually. The most intensive requirement is 3.2.1 – At least 95% of all staff have completed their annual Data Security Awareness Training in the last twelve months.

• 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)?
We are withholding this information under section 31.
The Trust has carefully considered all public interest arguments both in favour of disclosure and of maintaining the exemption. We have considered that it is vitally important to protect the security of our IT systems again criminal or malicious attack and that there is an extremely compelling interest in doing so. We do not believe that this is outweighed by the arguments in favour of openness and transparency in public sector organisations,

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:

Data Protection Officer
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