The Tavistock and Portman
NHS Foundation Trust

Freedom of Information Act 2000 disclosure log entry

Reference
23-24014

Date response sent
25/04/23

Subject
Cyber Security & Device Management

Details of enquiry
1. What is your primary inventory method for tracking each device type connected to the network?

    a. IT devices (i.e. pc, laptop)
    - CMDB
    - Manual spreadsheet
    - Automated device detection
    - Other
    - None

    b. IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
    - Not applicable. We do not use this equipment. None
    - CMDB
    - Manual spreadsheet
    - Automated device detection
    - Other
    - None

    c. Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
    - CMDB
    - Manual spreadsheet
    - Automated device detection
    - Other
    - None

    d. OT and building automation
    (i.e. heating and cooling, routers, switches)
    - CMDB
    - Manual spreadsheet
    - Automated device detection
    - Other
    - Non

e. 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

f. 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

g. 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

h. 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

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

a. 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:

b. How often is cybersecurity discussed by the board
   - Every 3 months
   - every 6 months
   - Every 12 months
   - Ad hoc
   - Never

c. Is medical device security a specific project on your roadmap for the next 12 months?
d. Are you able to respond to high severity NHS cyber alerts within the stated 48 hour timeline and patch within two weeks from disclosure?
e. What are the main challenges in meeting NHS Cyber Alert timelines?
f. What is your process for mapping individual NHS Cyber Alerts to every device on your network?
g. Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?
h. Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?
i. Are you able to attract and retain sufficient numbers of IT staff to fill available roles?
j. Do you feel you have sufficient IT staff to meet the demands placed upon you?
k. Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?
l. 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)?

Response sent

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

   a. IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
      Not applicable. We do not use this equipment. None

   b. Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
      None

   c. OT and building automation
      None

   d. How often is the information on those systems updated?
      As changes occur (real-time)

   e. IoT (i.e smart Tvs, smart watches,, assistants like Alexa, Siri)
      Not applicable. We do not use this equipment

f. Connected Medical devices / IoMT (i.e. remote health monitoring devices, robotic surgery, imaging machines, MRI scanner)
Not applicable. We do not use this equipment

h. OT and building automation (i.e. heating and cooling, routers, switches)
As changes occur (real-time)

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

a. What were the priorities discussed? (select all that apply)
Withheld under s31a of the Freedom of Information Act 2000 (FOIA)

b. How often is cybersecurity discussed by the board
Every 12 months, AND/OR Ad hoc

c. Is medical device security a specific project on your roadmap for the next 12 months?
Not applicable.

d. Are you able to respond to high severity NHS cyber alerts within the stated 48 hour timeline and patch within two weeks from disclosure?
-Yes, we meet majority of the alerts with in the timeline.

e. What are the main challenges in meeting NHS Cyber Alert timelines?
Balancing risk and impact to services

f. What is your process for mapping individual NHS Cyber Alerts to every device on your network?
Withheld under s31a of the Freedom of Information Act 2000 (FOIA)

g. Are you identifying and removing Chinese made devices recently banned for sensitive areas by the British Government? How are you identifying them?
No – None are known to exist on our network.

h. Does the Trust have enough resources to make sufficient investment to deal with replacing legacy and unsupported medical devices?
Not applicable. We are a mental health Trust and do not operate internet enabled medical devices – See our response to Question 1g above.

i. Are you able to attract and retain sufficient numbers of IT staff to fill available roles?
We have stable team, recruitment is a challenge in London

j. Do you feel you have sufficient IT staff to meet the demands placed upon you?
We are reviewing this to align with demand.

k. Approximately how long does it take for the Trust to assess on Data Security and Protection Toolkit (DSPT)? What takes the most time?
We do not hold this data. DSPT is an ongoing year-round activity.

l. 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)?
Withheld under s31a of the Freedom of Information Act 2000 (FOIA)
Response sent

Where recorded information is held, we have concluded that the exemption under s.31(a) of the FOIA *Law Enforcement: the prevention or detection* of crime is engaged. S.31(a) is a qualified exemption that requires the authority to carry out the public interest test. We have carried out the public interest test and have set out below the public interest arguments which we have considered:

Arguments in favour of disclosure:

- Promoting accountability and transparency on how public funds are utilised and spent

Arguments in favour of maintaining the exemption:

- The Trust has a duty to ensure that its information systems and assets are kept secure
- Disclosure of the requested information could facilitate criminal activity, in particular cybercrime, and especially when combined with other information already in the public domain or which could be gleaned from other sources, including any information that the Trust has previously provided or may be forced to disclose in the future.
- Disclosure of the requested information could, therefore, increase vulnerability to malicious attack, including the corruption, loss or non-availability of data or systems, which would impact on the Trust's ability to provide essential services
- These vulnerabilities could extend to suppliers on whose services the Trust relies.

We have concluded that, on balance, the public interest in maintaining the exemption outweighs the public interest in disclosure.