University Hospitals of North Midlands NHS Trust

Royal Stoke University Hospital
Data, Security and Protection
Newcastle Road
Stoke-on-Trent
Staffordshire
ST4 6QG

Email foi@uhnm.nhs.uk

Ref: FOIA Reference 2024/25-275

Date: 23rd August 2024

Dear Sir/Madam

I am writing to acknowledge receipt of your email dated 26th July 2024 requesting information under the Freedom of Information Act (2000) regarding cybersecurity

As of 1st November 2014 University Hospitals of North Midlands NHS Trust (UHNM) manages two hospital sites – Royal Stoke University Hospital, and County Hospital (Stafford). Therefore the response below is for the two sites combined from that date where appropriate.

Q1 How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)?

A1 The Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31
S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.
As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.
Factors in favour of confirming or denying the information is held
The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of ransomware attacks against the Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's ICT security.
Factors in favour of neither confirming nor denying the information is held
Cyber attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber attacks, and since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.
In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber attacks. Confirming or denying the type

iwl Committed to improving working lives of staff
Positive About Disabled People

of information requested would be likely to prejudice the prevention of cyber crime, and this is not in the public interest.
Balancing the public interest factors
The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the Trust is able to detect and deal with cyber attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's ICT systems.
The Trust determines that the balance of the public interest test lies in neither confirming or denying whether the information is held. This response should not be interpreted that the information requested is or is not held by the Trust.

In addition to the above:
I can neither confirm nor deny that the information you have requested is held by the Trust in its entirety. This is because the information requested in your question is exempt from disclosure under section 24(1) which states "Information which does not fall within section 23(1) is exempt information if the exemption from section 1(1) (b) 2 is required for the purpose of safeguarding national security." Furthermore withholding this information is also supported by the Freedom of Information Amendment (Terrorism and Criminal Intelligence) Act 2004

Q2 **For each of the following cyber incident types, please indicate if your organisation experienced them in any month from the 1st of July 2022- 1st of July 2024. If yes, specify the month(s) in which they occurred:**

- **Phishing attacks: Yes/No. If yes, which month(s)?**
- **Ransomware attacks: Yes/No. If yes, which month(s)?**
- **Distributed Denial of Service (DDoS) attacks: Yes/No. If yes, which month(s)?**
- **Data breaches: Yes/No. If yes, which month(s)?**
- **Malware attacks: Yes/No. If yes, which month(s)?**
- **Insider attacks: Yes/No. If yes, which month(s)?**
- **Cloud security incidents: Yes/No. If yes, which month(s)?**
- **Social engineering attacks (excluding phishing): Yes/No. If yes, which month(s)?**
- **Zero-day exploits: Yes/No. If yes, which month(s)**

A2 The Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here:
http://www.legislation.gov.uk/ukpga/2000/36/section/31
S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in

section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.
As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.
Factors in favour of confirming or denying the information is held
The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of ransomware attacks against the Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's ICT security.
Factors in favour of neither confirming nor denying the information is held
Cyber attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber attacks, and since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.
In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cyber crime, and this is not in the public interest.
Balancing the public interest factors
The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the Trust is able to detect and deal with cyber attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's ICT systems.
The Trust determines that the balance of the public interest test lies in neither confirming or denying whether the information is held. This response should not be interpreted that the information requested is or is not held by the Trust.

In addition to the above:
I can neither confirm nor deny that the information you have requested is held by the Trust in its entirety. This is because the information requested in your question is exempt from disclosure under section 24(1) which states "Information which does not fall within section 23(1) is exempt information if the exemption from section 1(1) (b) 2 is required for the purpose of safeguarding national security." Furthermore withholding this information is also supported by the Freedom of Information Amendment (Terrorism and Criminal Intelligence) Act 2004

Q3 **For each of the following supplier types, please indicate if any cyber incidents related to them occurred between the 1st of July 2022-1st of July 2024. If yes, specify the volume of cyber incidents that occurred:**

- **IT service providers: Yes/No**
- **Medical equipment suppliers: Yes/No**
- **Software vendors: Yes/No**
- **Cloud service providers: Yes/No**
- **Data storage/management companies: Yes/No**
- **Telecommunications providers: Yes/No**
- **Security service providers: Yes/No**
- **Managed service providers (MSPs): Yes/No**
- **Third-party payment processors: Yes/No**

A3 The Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here: http://www.legislation.gov.uk/ukpga/2000/36/section/31

S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.

As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.

Factors in favour of confirming or denying the information is held

The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of ransomware attacks against the Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's ICT security.

Factors in favour of neither confirming nor denying the information is held

Cyber attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber attacks, and since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber attacks. Confirming or denying the type of information requested would be likely to prejudice the prevention of cyber crime, and this is not in the public interest.

Balancing the public interest factors

The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the Trust is able to detect and deal with cyber attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to

enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's ICT systems.
The Trust determines that the balance of the public interest test lies in neither confirming or denying whether the information is held. This response should not be interpreted that the information requested is or is not held by the Trust.

In addition to the above:
I can neither confirm nor deny that the information you have requested is held by the Trust in its entirety. This is because the information requested in your question is exempt from disclosure under section 24(1) which states "Information which does not fall within section 23(1) is exempt information if the exemption from section 1(1) (b) 2 is required for the purpose of safeguarding national security." Furthermore withholding this information is also supported by the Freedom of Information Amendment (Terrorism and Criminal Intelligence) Act 2004

Q4 During the period from 1st of July 2022 -1st of July 2024, did your organisation experience any of the following impacts due to cyber incidents?

- **Were any appointments rescheduled due to cyber incidents? Yes/No**
- **Was there any system downtime lasting more than 1 hour? Yes/No**
- **Did any data breaches occur? Yes/No**
- **Were any patients affected by data breaches? Yes/No**

A4 The Trust can neither confirm nor deny whether information is held under section 31(3) of the FOIA. The full wording of section 31 can be found here:
http://www.legislation.gov.uk/ukpga/2000/36/section/31
S31(3) of the FOIA allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime.
As section 31(3) is a qualified exemption, it is subject to a public interest test for determining whether the public interest lies in confirming whether the information is held or not.
Factors in favour of confirming or denying the information is held
The Trust considers that to confirm or deny whether the requested information is held would indicate the prevalence of ransomware attacks against the Trust's ICT infrastructure and would reveal details about the Trust's information security systems. The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's ICT security.
Factors in favour of neither confirming nor denying the information is held
Cyber attacks, which may amount to criminal offences for example under the Computer Misuse Act 1990 or the Data Protection Act 1998, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber attacks, and since it holds large amounts of sensitive, personal and confidential information, maintaining the security of this information is extremely important.
In this context, the Trust considers that confirming or denying whether the requested information is held would provide information about the Trust's information security systems and its resilience to cyber attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber attacks. Confirming or denying the type

of information requested would be likely to prejudice the prevention of cyber crime, and this is not in the public interest.
Balancing the public interest factors
The Trust has considered that if it were to confirm or deny whether it holds the requested information, it would enable potential cyber attackers to ascertain how and to what extent the Trust is able to detect and deal with cyber attacks. The Trust's position is that complying with the duty to confirm or deny whether the information is held would be likely to prejudice the prevention or detection of crime, as the information would assist those who want to attack the Trust's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the Trust's systems, defences and possible vulnerabilities. This information would enter the public domain and set a precedent for other similar requests which would, in principle, result in the Trust being a position where it would be more difficult to refuse information in similar requests. To confirm or deny whether the information is held is likely to enable hackers to obtain information in mosaic form combined with other information to enable hackers to gain greater insight than they would ordinarily have, which would facilitate the commissioning of crime such as hacking itself and also fraud. This would impact on the Trust's operations including its front line services. The prejudice in complying with section 1(1)(a) is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's ICT systems.
The Trust determines that the balance of the public interest test lies in neither confirming or denying whether the information is held. This response should not be interpreted that the information requested is or is not held by the Trust.

In addition to the above:
I can neither confirm nor deny that the information you have requested is held by the Trust in its entirety. This is because the information requested in question (**) is exempt from disclosure under section 24(1) which states "Information which does not fall within section 23(1) is exempt information if the exemption from section 1(1) (b) 2 is required for the purpose of safeguarding national security." Furthermore withholding this information is also supported by the Freedom of Information Amendment (Terrorism and Criminal Intelligence) Act 2004

Q5 What percentage of your cybersecurity budget is allocated to each of the following supply chain security technologies? Please indicate the percentage for each:

- **Third-party risk assessment tools: ___%**
- **Vendor management systems: ___%**
- **Supply chain visibility and monitoring solutions: ___%**
- **Secure data sharing platforms: ___%**
- **Multi-factor authentication for supplier access: ___%**
- **Endpoint detection and response (EDR) for supplier systems: ___%**
- **API security solutions: ___%**

A5 We do not hold a specific cyber security budget so we are unable to respond to this question.

University Hospitals of North Midlands NHS Trust

*Please note that any individuals identified do not give consent for their personal data to be processed for the purposes of direct marketing.

UHNM NHS Trust is a public sector body and governed by EU law. FOI requestors should note that any new Trust requirements over the EU threshold will be subject to these regulations and will be advertised for open competition accordingly.

Where the Trust owns the copyright in information provided, you may re-use the information in line with the conditions set out in the Open Government Licence v3 which is available at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/. Where information was created by third parties, you should contact them directly for permission to re-use the information.

An anonymised copy of this request can be found on the Trust's disclosure log, please note that all requests can be found at the following link: http://www.uhnm.nhs.uk/aboutus/Statutory-Policies-and-Procedures/Pages/Freedom-of-Information-Disclosure-Log.aspx

This letter confirms the completion of this request. A log of this request and a copy of this letter will be held by the Trust.

If you have any queries related to the response provided please in the first instance contact my office.

Should you have a complaint about the response or the handling of your request, please also contact my office to request a review of this. If having exhausted the Trust's FOIA complaints process you are still not satisfied, you are entitled to approach the Information Commissioner's Office (ICO) and request an assessment of the manner in which the Trust has managed your request.

The Information Commissioner may be contacted at:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or via www.ico.org.uk.

Yours,

Rachel Montinaro
Data Security and Protection Manager - Records

iwl Committed to improving working lives of staff

Positive About Disabled People