NHS
North East and
North Cumbria

Our Reference North East and North Cumbria ICB\
FOI ICB 24–195

NECS – John Snow House
Durham University Science Park
Durham
DH1 3YG

Tel: 0191 301 1300
E-mail: necsu.icbfoi@nhs.net

By Email

8 August 2024

Dear Applicant

Freedom of Information Act 2000 – Request for Information – NHS North East and North Cumbria Integrated Care Board (NENC ICB)

Thank you for your request received by North of England Commissioning Support (NECS) on 1 August 2024 for information held by NHS North East and North Cumbria Integrated Care Board (the ICB) under the provisions of the Freedom of Information Act 2000.

The ICB covers the areas of County Durham, Gateshead, Newcastle, North Cumbria, North Tyneside, Northumberland, South Tyneside, Sunderland, and Tees Valley (which covers the five local authorities of Darlington, Hartlepool, Middlesbrough, Redcar and Cleveland and Stockton-on-Tees).

Please find the information you requested on behalf of the ICB as follows.

Your Request

I am writing to submit a request for information under the Freedom of Information Act 2000 (FOIA). My request is as follows:

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

2. 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)

3. 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

4. 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

5. 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: ___%

If it looks like the work involved in responding to this FOI will exceed the time permitted under this FOIA, please contact me as soon as possible to discuss how I can reduce this request's scope.

If you have any questions or need more clarification, please contact me.

Our Response

The ICB 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.

Application of the Public Interest Test if required
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 ICB considers that to confirm or deny whether the requested information is held would indicate the prevalence of cyber- attacks against the ICB's ICT infrastructure and would reveal details about the ICB's information security systems. The ICB recognises that answering the request would promote openness and transparency with regards to the ICB'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 2018, are rated as a Tier 1 threat by the UK Government. The ICB, 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 ICB considers that confirming or denying whether the requested information is held would provide information about the ICB's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the ICB'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 cybercrime, and this is not in the public interest.

If the ICB were either to confirm or deny the existence of the requested information, the disclosure would be likely to prejudice the effective conduct of public affairs for the ICB, the NHS or any other government department(s) and as such conflicts with Section 36(2c) of the FOIA. The full wording of section 36 can be found here: https://www.legislation.gov.uk/ukpga/2000/36/section/36

Balancing the public interest factors
The ICB 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 extend the ICB is able to detect and deal with ICT security attacks. The ICB'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 ICB's ICT systems. Disclosure of the information would assist a hacker in gaining valuable information as to the nature of the ICB'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 ICB 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 ICB's operations including its front-line services. The prejudice in complying with section 31(1)(a) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the ICB's ICT systems.

In accordance with the Information Commissioner's directive on the disclosure of information under the Freedom of Information Act 2000 your request will form part of our disclosure log. Therefore, a version of our response which will protect your anonymity will be posted on the NHS ICB website https://northeastnorthcumbria.nhs.uk/.

If you have any queries or wish to discuss the information supplied, please do not hesitate to contact me on the above telephone number or at the above address.

If you are unhappy with the service you have received in relation to your request and wish to request a review of our decision, you should write to the Senior Governance Manager using the contact details at the top of this letter quoting the appropriate reference number.

If you are not content with the outcome your review, you do have the right of complaint to the Information Commissioner as established by section 50 of the Freedom of Information Act 2000. Generally, the Information Commissioner cannot make a decision unless you have exhausted the complaints procedure provided by the North of England Commissioning Support Unit.

The Information Commissioner can be contacted at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

www.ico.org.uk

Any information we provide following your request under the Freedom of Information Act will not confer an automatic right for you to re-use that information, for example to publish it. If you wish to re-use the information that we provide and you do not specify this in your initial application for information then you must make a further request for its re-use as per the Re-Use of Public Sector Information Regulations 2015 www.legislation.gov.uk . This will not affect your initial information request.

Yours sincerely

S Davies

S Davies
Information Governance Officer