NHS
North East and
North Cumbria

Our Reference North East and North Cumbria ICB\
FOI ICB 24–215

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

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

By Email

5 September 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 22 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 occurred in the last two years (1st of July 2022 – 1st of July 2024)? Please provide separate information on:
   - Cyber incidents that occurred within the NHS North East and North Cumbria ICB
   - Cyber incidents NHS North East and North Cumbria ICB reported to NHS England
2. During the period from 1st of July 2022 – 1st of July 2024, please provide accurate information on or the closest estimates for:
   - The number of rescheduled patient appointments due to cyber incidents.
   - The number of incidents that were a result of human error.
   - The duration of any system downtime caused by the incident.
   - The number of data breaches that occurred.
   - The number of patients affected by data breaches.

3. What percentage of your organisation's total training budget is allocated to cybersecurity-related training for the current fiscal year? ___%
4. Does your organisation have a formal cybersecurity skills assessment process to identify skill gaps among employees? (Yes/No) If yes, please provide information on:
   a. A description of the assessment methodology.
   b. The frequency with which these assessments are conducted.
   c. How the results of these assessments inform training initiatives.
5. Has your organisation implemented specific measures to address and mitigate cybersecurity risks associated with human error? (Yes/No) If yes, please provide information on:
   a. Targeted training programmes.
   b. Awareness campaigns.
   c. Any technological solutions implemented to reduce the risk of human error.

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

We can confirm, as per Section 1(1) of the Freedom of Information Act 2000, the ICB holds some of the information you have requested.

1. Cyber incidents in the last two years (1st of July 2022 – 1st of July 2024):
   - The ICB did not experience any incidents which is considered Cyber related.
   - The ICB, on behalf of constituent partners, raised 1 cyber incident to NHS England.
2. On this occasion it is not possible to provide the requested information. In line with your rights under section 1(1)(a) of the Act to be informed whether information is held, we confirm the ICB does not hold any of the information requested.
3. Cyber security is part of statutory and mandatory training for all staff; however, NENC ICB does not measure the specific budget allocation for this purpose.
4. Yes, NENC ICB has a formal cybersecurity skills assessment process to identify skill gaps among employees.
   a. The assessment methodology is online mandatory training.
   b. Assessments are conducted annually.
   c. Results are considered as part of future training needs.
5. Yes, NENC ICB has implemented specific measures to address and mitigate cybersecurity risks associated with human error.
   a. Targeted training programmes are not carried out.
   b. Awareness campaigns are carried out.
   c. Technological solutions implemented to reduce the risk of human error are carried out.

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 faithfully

S Davies

S Davies
Information Governance Officer