University Hospitals of North Midlands NHS Trust

Royal Stoke University Hospital
Quality, Safety and Compliance Department
Newcastle Road
Stoke-on-Trent
Staffordshire
ST4 6QG

Email foi@uhnm.nhs.uk

Ref: FOIA Reference 2018/19-708

Date: 16th April 2019

Dear
I am writing in response to your email dated 20th February 2019 requesting information under the Freedom of Information Act (2000) regarding Cyber Security. I apologise for the delay in responding.

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 questions 4 and 5 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

In addition to the above exemption, UHNM can neither confirm nor deny whether the information you have requested in question 3 as this is not held centrally, this is recorded in multiple systems, and in some cases, the retention period is considerably less than the requested periods. In order to confirm whether this information is held we would therefore have to individually access the records within each system and extract the information where it is present. We therefore estimate that complying with your request is exempt under section 12 of the FOI Act: *cost of compliance is excessive*. The section 12 exemption applies when it is estimated a request will take in excess of 18 hours to complete. We estimate that accessing and reviewing all records and then extracting relevant information would take longer than the 18 hours allowed for.

Under section 16 of the FOI Act we are required to provide requestors with advice and assistance where possible. We would therefore like to advise you that if your request is shortened to exclude questions 3, 4 and 5 we are able to comply within the 18 hour time frame. In order to avoid delay to your response we have provided this below.

On 13th March 2019 we contacted you via email as we required a time frame for questions 2, 4 and 5.

On 3rd April 2019 you replied via email the following:
"Please could you provide answers for Q2, 4 and 5 for the time period of 2017-2018 inclusive?"

On the same day we replied that we also required clarification on what you classified as a Cyber-attack (Q3)

On 4th April 2019 you replied via email the following:
"*We would define a cyberattack as any malicious attempt to damage or infiltrate your computer network/systems. These would include ones that you have detected and prevented, as well as those that have succeeded or made an impact in any way*."

University Hospitals of North Midlands NHS Trust

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 Are you aware of the Minimum Cyber Security Standard, published 25th June 2018?

a. Yes
b. No

A1 Yes

Q2. What is your annual dedicated budget for cybersecurity (including personnel and technology)?

a. £10,000 or less
b. £10,001 - £50,000
c. £50,001 - £100,000
d. £100,001 - £500,000
e. £500,001 - £1,000,000
f. £1,000,001 - £5,000,000
g. £5,000,001 - £10,000,000
h. £10,000,001 or more

A2 UHNM does not have a budget heading (Cyber) as this is part of a wider ICT budget and therefore we are unable to split this out.

Q3 Approximately how many cyber-attacks (of any kind) have you experienced in your organisation in these 12-month periods?

	None	1 – 50	50 – 100	100 – 200	200 – 500	500 - 1000	1000+
1st January 2017 – 31st December 2017							
1st January 2018 – 31st December 2018							

A3 Section 12 exemption as detailed above.

Q4 Which of the following attack / cybersecurity threat types have been detected by your organisation? [Select all that apply]

a. Hacking
b. Phishing
c. Malware
d. Ransomware
e. Accidental/careless insider threat
f. Malicious insider threat

g. **Foreign governments**
h. **Crypto mining**
i. **Other, please specify: _____**

A4 Section's 23 and 24 exemptions as detailed above.

Q5 Which of the following form part of your cybersecurity defence technology strategy? [Select all that apply]

a. **Firewall**
b. **Antivirus software**
c. **Network device monitoring**
d. **DNS filtering**
e. **Malware protection**
f. **Log management**
g. **Network configuration management**
h. **Patch management**
i. **Network traffic analysis**
j. **Multi-factor authentication**
k. **Network perimeter security solutions**
l. **Employee training (whole organisation)**
m. **Employee training (IT team)**
n. **Other, please specify: ____**

A5 Section's 23 and 24 exemptions as detailed above.

Q6 Which of these obstacles has your organisation experienced in maintaining or improving IT security? [Select all that apply]

a. **Competing priorities and other initiatives**
b. **Budget constraints**
c. **Lack of manpower**
d. **Lack of technical solutions available at my agency**
e. **Complexity of internal environment**
f. **Lack of training for personnel**
g. **Inadequate collaboration with other internal teams or departments**
h. **Other, please specify: _____**

A6 The FOI Act (2000) is for the release of information that is held/recorded and does not cover the opinions of persons regarding suppliers, systems or procedures, therefore this information is not held.

*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.

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.

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.

If following review of the responses I can be of any further assistance please contact my secretary on 01782 676474.

Yours,

R Carlisle

Leah Carlisle
Deputy Head of Quality, Safety & Compliance