



Ref: FOIA Reference 2021/22-407

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

Date: 10<sup>th</sup> January 2022

Email [foi@uhnm.nhs.uk](mailto:foi@uhnm.nhs.uk)

Dear

I am writing to acknowledge receipt of your email dated 16<sup>th</sup> November 2021 requesting information under the Freedom of Information Act (2000) regarding counter fraud.

On the same day we contacted you via email as we required the following clarification:

**Q1 responsibility for auditing/monitoring insider threats** – against what? what you are asking for? are you talking threats to computer systems or if we have a local counter fraud specialist?

On 25<sup>th</sup> November 2021 you replied via email with the following:

*'Firstly may I apologise for the delay in responding to your email. For some reason your email went into my 'junk email'. I would like to know if anyone within your organisation has an overall responsibility for auditing/monitoring insider threats – i.e. threats posed by employees working within the organisation and not external threats from such events as hacking or phishing emails. From other responses, that the responsibility sits with the Director of Digital or Director of Finance and for others they have Internal Audit and Counter Fraud Teams.'*

As of 1<sup>st</sup> 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 Does anyone in University Hospitals of North Midlands NHS Trust have responsibility for auditing/monitoring insider threats – counter fraud?**

A1 We have a combination of systems and people to limit the impact and likelihood of counter fraud.

**Q2 How is University Hospitals of North Midlands NHS Trust able to check that your systems are being used in the way that they should?**

A2 There are systems that monitor and alert to any potential abnormal usage

**Q3 How many employees have misused their authority and used your IT systems inappropriately, (e.g.: to identify vulnerable people, falsify records etc) in the last 5 years?**

A3 One 'incident was reported where employees have misused their authority and used our IT systems inappropriately (e.g. to identify vulnerable people, falsify records etc.) in the last 5 years'.

**Q4 How much money has University Hospitals of North Midlands NHS Trust lost as a result of insider fraud/corruption in the last 5 years? (NHS Counter Fraud Authority estimate that the NHS is vulnerable to £1.21 billion worth of fraud each year and I would like to understand how that relates to University Hospitals of North Midlands NHS Trust).**

A4 None

**Q5 How often do you have to audit your IT systems to make sure employees are using them appropriately?**

A5 There is no defined 'have to' frequency in terms of auditing; High risk events are routinely monitored. And various monthly spot checks are carried out.

**Q6 When and how would University Hospitals of North Midlands NHS Trust be alerted to the fact that someone has used the IT system inappropriately?**

A6 As per regular tasks referenced in Q5, in addition we have processes for internal reporting of incidents (DATIX), whistle blowing process & process for addressing concerns raised by any staff, patients, relatives etc.

**Q7 Who has overall responsibility for ensuring that your IT systems are secure from internal threats?**

A7 Overall responsibility sits with the Director of Digital Transformation but delegated to Lead Cyber Engineer.

**Q8 Do you currently have a budget allowance for auditing and monitoring your IT systems within University Hospitals of North Midlands NHS Trust? If so, how much?**

A8 We are unable to provide, as this is part of a wider budget

**Q9 How many computers are there in University Hospitals of North Midlands NHS Trust?**

A9 8843

**Q10 What operating systems do your computers use?**

A10 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 Council 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 ICT security 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.

#### **Q11 How many staff are employed at University Hospitals of North Midlands NHS Trust?**

A11 As at 31<sup>st</sup> October 2021, the headcount of fixed term and permanent employees was 11425

\*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.

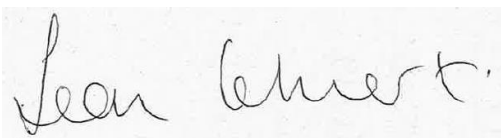
Should you have a complaint about the response or the handling of your request, please also contact my office to request a review of this. If having exhausted the Trust's FOIA complaints process you are still not satisfied, you are entitled to approach the Information Commissioner's Office (ICO) and 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](http://www.ico.org.uk).

If following review of the responses I can be of any further assistance please contact my secretary on 01782 671612.

Yours,



Jean Lehnert  
**Data, Security & Protection Manager**