

Ref: FOI/GS/ID 9304

**Please reply to:**  
FOI Administrator  
Trust Management  
Maidstone Hospital  
Hermitage Lane  
Maidstone, Kent  
ME16 9QQ  
Email: [mtw-tr.foiadmin@nhs.net](mailto:mtw-tr.foiadmin@nhs.net)  
[www.mtw.nhs.uk](http://www.mtw.nhs.uk)

20 November 2024

## **Freedom of Information Act 2000**

I am writing in response to your request for information made under the Freedom of Information Act 2000 in relation to Cyber Security.

*You asked: All questions are shown as received by the Trust.*

*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: \_\_\_%*

Trust response:

The Trust has a dedicated Cyber Security team and has purchased and installed many different solutions to help protect us against cyber threats.

Following the Synnovis cyber-attack on the NHS, the Trust has taken the decision to not release information relating to its Cyber security.

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 cyber- attacks against the Trust's infrastructure and the level of detail poses a number of risks in respect of security and information.

The Trust recognises that answering the request would promote openness and transparency with regards to the Trust's software systems. 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 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 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 cybercrime, and this is not in the public interest.

Balancing the public interest factors:

The NHS 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 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 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) FOIA is real and significant as to confirm or deny would allow valuable insight into the perceived strengths and weaknesses of the Trust's systems.