NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Direct Line: 01623 672232
Our Ref: 53424
E-mail: sfh-tr.foi.requests@nhs.net

King's Mill Hospital
Mansfield Road
Sutton in Ashfield
Nottinghamshire
NG17 4JL

Tel: 01623 622515
Join today: www.sfh-tr.nhs.uk

[redacted]

RE: Freedom of Information Request

12th December 2023

Dear Sir/Madam

With reference to your request for information received on 2nd October 2023, I can confirm in accordance with Section 1 (1) of the Freedom of Information Act 2000 that we do hold the information you have requested. A response to each part of your request is provided below.

In your request you asked:

1. **In 2023, what annual cybersecurity budget has been allocated to your NHS Trust?**
   £300k Capital allocation.

2. **Can you also provide your Trust's annual cybersecurity budget for the years:**
   a. **2022 -** £300k
   b. **2021 -** £300k
   c. **2020 -** £300k
   d. **2019 -** £299k
   e. **2018 -** No dedicated Cyber budget, however Capital Plan covered Cyber initiatives as required.
   f. **2017 -** No dedicated Cyber budget, however Capital Plan covered Cyber initiatives as required.

3. **In 2023, how is your annual cybersecurity budget spent:**
   a. **What percentage goes towards cybersecurity training for employees?**
   b. **What percentage goes towards technology investments?**
   c. **What percentage goes towards employee resources for your cybersecurity team?**
   The Trust receive a Cyber Security Service from Nottinghamshire Health Informatics Service, however this is a part of a block NHS contract and it is not possible to break out cyber specific spends.

4. **How many employees work in your NHS Trust?**
   Substantive Staff – 5,896
   Bank Staff – 2,052

5. **How many employed, full-time members of staff make up your NHS Trust's cyber/infosecurity team?**
   The Trust receive a Cyber Security Service from Nottinghamshire Health Informatics Service, however this is a part of a block NHS contract and it is not possible to break out cyber specific staff supporting just Sherwood Forest Hospitals NHS Foundation Trust.

6. **How many hours of cybersecurity training are employees of your NHS Trust required to undertake every year?**
   All staff are required to complete mandatory Information Governance Training every year which covers cybersecurity.

7. **Has your NHS Trust paid any ransom demands to cybercriminals in the last five years?**
   a. **If yes, how much did you pay in total?**

Section 31 - Cyber Security

The organisation has a dedicated Cyber Security Team and has purchased and installed many different solutions to help protect us against cyber threats. However, we will not be publicising or sharing the details of these products, solutions or vendors because we believe that in doing so, we put our self at risk.

We will also not be publishing details around any system be it hardware or software that is either end of life or is coming to end of life as we believe that publishing this information also puts the Trust at risk. This would include but is not limited to items such as "does the trust have any machines running an out of date operating system or unsupported hardware". Publication of Information relating to the organisation's provision of cyber security software, hardware and web based solutions, could lead to those who wish to undertake any cyber attack or expose the potential for such actions to be taken by other bad actors.

Working collaboratively with the advice from national and local collaboration, the organisation has taken the view that to share such information in its broadest sense could potentially jeopardise our security provision, and inadvertently lead to a significant risk of data leakage, data loss, loss of public trust and confidence in services, and associated fines under Data Protection legislation.

With this in mind, the organisation considers that this information is exempt under Section 31 of the FOI Act for the following reasons:
The organisation 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. 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.

In this context, providing requested information would provide information about the organisation's information security systems and its resilience to cyber-attacks. There is a very strong public interest in preventing our information systems from being subject to cyber-attacks. Providing the type of information requested would be likely to provide attackers with information relating to the state of our cyber security defences, and this is not in the public interest.

8. **Has your NHS Trust had any patient records compromised / stolen by cybercriminals in the last five years?**
   a. If yes, how many records were compromised / stolen?
   Section 31 – Please see Q7

I trust this information answers your request. Should you have any further enquiries or queries about this response please do not hesitate to contact me. However, if you are unhappy with the way in which your request has been handled, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Sally Brook Shanahan, Director of Corporate Affairs, King's Mill Hospital, Mansfield Road, Sutton in Ashfield, Nottinghamshire, NG17 4JL or email sally.brookshanahan@nhs.net.

If you are dissatisfied with the outcome of the internal review, you can apply to the Information Commissioner's Office, who will consider whether we have complied with our obligations under the Act and can require us to remedy any problems. Generally, the Information Commissioner's Office cannot decide unless you have exhausted the internal review procedure. You can find out more about how to do this, and about the Act in general, on the Information Commissioner's Office website at: https://ico.org.uk/your-data-matters/official-information/.

Complaints to the Information Commissioner's Office should be sent to FOI/EIR Complaints Resolution, Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Telephone 0303 1231113, email casework@ico.org.uk.

If you would like this letter or information in an alternative format, for example large print or easy read, or if you need help with communicating with us, for example because you use British Sign Language, please let us know. You can call us on 01623 672232 or email sfh-tr.foi.requests@nhs.net.

Yours faithfully

Information Governance Team