Healthier Communities, Outstanding Care

Sherwood Forest Hospitals
NHS Foundation Trust

Direct Line: 01623 672232
Our Ref: 173
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

14th August 2024

[redacted]

Dear Sir/Madam

Freedom of Information Act (FOI) 2000 - Request for Information Reference: cybersecurity of the UK government

I am writing in response to your request for information under the FOI 2000.

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.

FOI Request / Question	Question Response	Is there an exemption?	Exemption	Exemption Details
1. **How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)?**		Yes	NHIS CYBER	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.
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**				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.
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: ___%**				

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