Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI202425/191
From: Private Individual

Date: 05 August 2024

Subject: Cyber Security Incidents

Q1 How many cyber incidents (threat and breach) occurred in the last two years (1st of July 2022-1st of July 2024)?

A1 None

Q2 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:
a. Phishing attacks: Yes If yes, which month(s)?
b. Ransomware attacks: Yes If yes, which month(s)?
c. Distributed Denial of Service (DDoS) attacks:
d. Data breaches: Yes. If yes, which month(s)?
e. Malware attacks: Yes If yes, which month(s)?
f. Insider attacks:
g. Cloud security incidents:
h. Social engineering attacks (excluding phishing):
i. Zero-day exploits: Yes If yes, which month(s) -

A2 Information exempt under s31 – law enforcement, specifically section 31 (1) (a) relating to the prevention and detection of crime.

We have assessed the public interest in disclosure and believe the only factor for release would be openness and transparency, however the factors against release clearly outweigh this as release of the information would place the Trusts information systems and other related assets at risk of attack from hackers if released into the public domain. This would have a major impact on the Trusts ability to maintain confidentiality, integrity and availability of systems and information and would severely disrupt services to our patients and would have a substantial impact on the Trusts reputation therefore causing financial loss and would damage the Trusts commercial interests.

Q3 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:
a. IT service providers:
b. Medical equipment suppliers:
c. Software vendors:
d. Cloud service providers:
e. Data storage/management companies:
f. Telecommunications providers:
g. Security service providers:
h. Managed service providers (MSPs):
i. Third-party payment processors:

A3 Information not held – zero for all supplier types.

Q4 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?
a. Were any appointments rescheduled due to cyber incidents?
b. Was there any system downtime lasting more than 1 hour?
c. Did any data breaches occur?
d. Were any patients affected by data breaches?

A4
a. No
b. No
c. No
d. No

Q5 What percentage of your cyber security budget is allocated to each of the following supply chain security technologies? Please indicate the percentage for each:
a. Third-party risk assessment tools: ___%
b. Vendor management systems: ___%
c. Supply chain visibility and monitoring solutions: ___%
d. Secure data sharing platforms: ___%
e. Multi-factor authentication for supplier access: ___%
f. Endpoint detection and response (EDR) for supplier systems: ___%
g. API security solutions: ___%

A5 Information not held – breakdown of the cyber security budget not held to the level above.