Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI202526/092
From: Commercial

Date: 02 June 2025

Subject: Cyber Security Incidents and Measures (FY22–FY25)

Q1 Ransomware incidents (FY2022–FY2025)
Please confirm whether any digital systems within hospitals managed by your NHS Trust were affected by ransomware attacks during the financial years 2022–2023 through to 2024–2025 (inclusive).
If yes:
- How many separate ransomware incidents occurred within this period?
- For each incident, please provide:
  - The date or month of occurrence
  - A brief description of the nature of the attack (e.g. type of ransomware, point of system entry, services impacted)

A1 Zero

Q2 Data breaches following cyber incidents (FY2022–FY2025)

Were any data breaches reported as a result of ransomware or other cyber incidents during this period?

If yes, please provide for each breach:
- The type(s) of data affected (e.g. patient records, staff information)
- The specific impacts of each breach, categorised as follows (where applicable):
  - Loss of patient data
  - Loss of staff data
  - Disruption to patient services (please specify which services, if known)
  - Disruption to operational processes
  - Financial impact (e.g. cost of recovery, penalties, compensation, etc.)
  - Other impacts – please specify

A2 Yes, this information is exempt under Section 21 of the Freedom of Information Act 2000 - 'Information reasonably accessible to the applicant by other means'.

This information is available on our website, it can be found here Liverpool Heart and Chest Hospital | NEWS: Cyber Issue Latest

Q3 Current cyber security measures (as of date of request)

Please list all cyber security measures and protocols currently in place across the Trust. These may include, but are not limited to:
- Cyber insurance (including provider and coverage if available)
- Internal and external firewall systems
- Use of multi-factor authentication (MFA) for user accounts
- Access control systems for sensitive data and critical systems

- Anti-virus and anti-malware protection
- Cyber security training or awareness programmes for employees
- Regular penetration testing or security audits (please specify frequency)
- Existence and status of an incident response plan (e.g. last updated date)

A3 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.