Mersey and West Lancashire
Teaching Hospitals
NHS Trust

Ref. No:	1799
Date:	03/06/25
Subject:	Cyber Security Incidents and Measures (FY22–FY25)

REQUEST

1. 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)

2. 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

3. 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)

RESPONSE

The information is exempt from disclosure under the Freedom of Information Act.

Section 31(1)(a) of the Act states:

> 31. Law enforcement.
> (1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—
> (a) the prevention or detection of crime,

Guidance from the Information Commissioner's Office states:

> *Section 31(1)(a) will cover all aspects of the prevention and detection of crime…The exemption also covers information held by public authorities without any specific law enforcement responsibilities…It could also be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime for example, by disclosing its own security procedures*

Information disclosed under Freedom of Information becomes publically available. This means that the impact of disclosure must be considered from the general release of information and not limited to disclosure to one individual (the requestor).

The Trust determines that to disclose this would prejudice the security of the systems by allowing for the assessment of the Trust's security procedures and where, if any, vulnerabilities exist. Consequently section 31 (1) (a) is being applied to this request.