

## FOI 0106/2025 Response

### 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)

There have been NIL (0) ransomware attack

### 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

NIL (0)

### 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)**

We use all the following measures:

- 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
- Managed detection and response
- Cyber security training or awareness programmes for employees
- Regular penetration testing or security audits
- Current incident response plan (e.g. last updated 04/2025)
- Cannot confirm or deny whether we have cyber insurance