Ref. No:	2138
Date:	29/10/25
Subject:	Legacy Clinical Systems used for Data Storage

REQUEST

On Legacy Clinical Systems used for Data Storage within the Trust.

'**An NHS legacy clinical system is an outdated or unsupported/supported technology used for storing and processing patient data and records. These older systems are often deeply embedded in hospital workflows but pose challenges for data storage, including limited interoperability, security risks, and high maintenance costs**. '

1. Does the Trust use legacy clinical systems for data storage, e.g. Read-only systems that are only used for patient data storage

2. If yes, please provide the name of the

   - **System/s**
   - **Supplier/s**
   - **Current contract end date/s**

3. Is this system used Trust wide or for a limited number of departments?

4. Please provide list of departments system is used?

5. What is the total annual licence cost of these systems per annum?

6. If service contracts are in place, what are the total annual costs cumulatively?

RESPONSE

Freedom of Information Request – Response

Mersey and West Lancashire Teaching Hospitals NHS Trust has considered your request and has concluded that it is unable to confirm or deny whether it holds the information you have requested. This decision is made under the following exemptions of the Freedom of Information Act 2000:

- **Section 24(2)** – National Security

- **Section 38(2)** – Health and Safety

Both exemptions are **prejudice-based and qualified**, meaning the Trust must demonstrate the potential harm in confirming or denying the existence of the information and assess the public interest.

Harm in Confirming or Denying Whether the Information is Held

Confirming whether specific IT security information is held could compromise the effectiveness of the Trust's protective measures. Disclosure of details such as product names, suppliers, contract terms, costs, or technical descriptions may enable malicious actors to identify vulnerabilities within our infrastructure.

This could expose the Trust—and potentially the wider NHS—to cyber threats, including attacks from criminals or terrorists. Such exposure would pose a significant risk to the safety of patients and staff, and undermine the integrity of NHS services.

Public Interest Test

Factors Favouring Disclosure

- Enhancing transparency around public sector spending and procurement.
- Increasing public understanding of the Trust's approach to IT security.

Factors Favouring Non-Disclosure

- Protecting the security and resilience of NHS infrastructure.
- Preventing the identification of potential vulnerabilities.
- Safeguarding the health and safety of patients and staff.
- Maintaining public confidence in the NHS's ability to provide secure and effective care.

Conclusion

While there is public interest in transparency, the risks associated with confirming whether the requested information is held outweigh the benefits. Disclosure could compromise national security and endanger the safety of individuals.

Therefore, in accordance with Sections 24(2) and 38(2) of the Freedom of Information Act, the Trust will neither confirm nor deny whether it holds the information requested.