Mersey and West Lancashire
Teaching Hospitals
NHS Trust

Ref. No:	2002
Date:	19/08/25
Subject:	Access to Clinical Information Systems

REQUEST

1. **Access to Testing Clinical Information Systems**
    1. What is the approval process by which an external organisation may apply or request to connect with the trust's **test clinical systems of record**. (e.g. EMR, EHR, PACS)
    2. Which internal teams, roles, or committees are responsible for approving such a connection?
    3. What steps are involved in obtaining the necessary permissions or agreements to establish such a connection?
    4. What is the entry point for this process? e.g. email address or webform.
1. **Access to Production Clinical Information Systems**
    1. What is the approval process by which an external organisation may apply or request to connect with the trust's **production clinical systems of record**. (e.g. EMR, EHR, PACS)
    2. Which internal teams, roles, or committees are responsible for approving such a connection?
    3. What steps are involved in obtaining the necessary permissions or agreements to establish such a connection?
    4. What is the entry point for this process? e.g. email address or webform.

Clarity on the abbreviations below.

API – Application Programming Interface
EHR – Electronic Health Record
EMR – Electronic Medical Record
FHIR – Fast Healthcare Interoperability Resources
GP – General Practitioner
PACS – Picture Archiving and Communication System
SME – Small and Medium-sized Enterprise

RESPONSE

Thank you for your request regarding access to the Trust's clinical information systems, including both test and production environments (e.g. EMR, EHR, PACS). While we understand the importance of transparency and collaboration, the Trust must also prioritise the security and integrity of its systems and the protection of patient data.

In accordance with the Freedom of Information Act 2000, the Trust is applying an exemption under Section 31(1)(a) – Law Enforcement, which states:

"Information is exempt if its disclosure would, or would be likely to, prejudice the prevention or detection of crime."
This exemption is supported by guidance from the Information Commissioner's Office, which clarifies that Section 31(1)(a) applies not only to law enforcement bodies but also to any public authority where disclosure could increase vulnerability to crime. In this case, releasing details about how external organisations may request access to clinical systems, whether test or live, would expose the Trust's internal security procedures and potentially highlight areas of vulnerability.

It is important to note that information disclosed under the Freedom of Information Act becomes publicly available. Therefore, MWL must consider the impact of general release, not just disclosure to the individual requester. Revealing the approval process, responsible teams, and entry points for system access could enable malicious actors to exploit or target the Trust's infrastructure.

As such, the Trust has determined that disclosing whether external organisations can access clinical systems, and the process by which this might occur, would likely prejudice the security of those systems. This includes both test environments, which often mirror production systems, and live clinical systems that contain sensitive patient data.

Consequently, the Trust is applying Section 31(1)(a) to withhold this information. This decision reflects our commitment to safeguarding patient information, maintaining system integrity, and complying with national data protection and cybersecurity standards.