**LAMBETH TOGETHER**
**Lambeth Q&A response**

## Q&A RESPONSES* 1

1. ***What, if any, measures did Synnovis put in place following the attacks on SYNLAB French and Italian subsidiaries? (Synnovis response)***

   For security reasons, and especially given the recent incident, we do not comment on the specifics of our IT systems or security protocols, however, we can confirm several of the steps taken to further secure our infrastructure and implement operational mitigations for partners of Synnovis here in the UK. These have included but are not limited to:

   - Working with a taskforce of IT experts from Synnovis and the NHS, together with third-party advisers
   - Implementing a completely new cloud infrastructure environment, using CIS Benchmark standards
   - Enhancing governance policies and procedures across all platforms (including resetting all service platform passwords and expiring MFA tokens)
   - Compliance with NCSC infrastructure requirements and security principles
   - External penetration testing.

   At a Group level, SYNLAB constantly improves security measures and emergency processes as they are vital components in responding to and mitigating cyber-attacks on essential healthcare providers. It follows a "Zero Trust" approach, which is being continuously implemented. This includes ongoing investments in the security of its IT systems and processes, as well as employee awareness to protect its infrastructure and data.

2. ***Is Synnovis' IT system compliant with SEL ICS' Cyber Security strategy? (Trust Response)***

   The Synnovis IT system is currently being restored and has been and will be subject to a variety of changes as part of this process. The Trusts will therefore assess the Synnovis IT system's overall compliance with the new SEL ICS strategy when this work has been completed.

3. ***What are the Data protection implications of the cyber attack? (Synnovis response)***

   As required the attack has been disclosed by the Trust to the Information Commissioner .

   On 1 July (Update on Cyber Incident: 01 July 2024 | Synnovis), Synnovis confirmed that its initial analysis of the published stolen data found:

   - The format in which it has been published represents a partial copy of content from Synnovis' administrative working drives. This drive held information which supported our corporate and business support activities.



**1 This document contains responses and statements provided by multiple parties. The Trusts have contributed solely to responses numbered 2, 4, 5,6,7,8,9 and 10, and have not verified and bear no responsibility for the viewpoints expressed by other parties in other responses*

- In some circumstances this information may contain personal data such as names, NHS numbers and test codes (identifying the requested test), although analysis is ongoing.
- Synnovis personnel files and payroll information were not published, but more needs to be done to review other data that has been published relating to our employees.
- The format and partial nature of what has been published makes it complex to interpret. As is typical in such incidents, it will take some time to conduct a comprehensive analysis in order to identify the full nature of the impacted data, organisations and individuals.

The interrogation of the stolen data is advanced, ongoing and conducted with the support of national bodies and technical specialists.

The investigation timeframe, in keeping with the scale and scope of such an incident, is in line with the time required to thoroughly conclude which individuals or organisations have been impacted. Synnovis will communicate with the relevant parties as soon as it is appropriate and responsible to do so. Arrangements are in place so that the relevant parties are briefed, in line with applicable obligations, so that they can consider whether they need to notify their data subjects.

Synnovis is very aware of the impact and upset this incident has caused to patients, service users and frontline NHS colleagues and is truly sorry for the frustration and concern caused by the action of these cybercriminals.

Further information is available at Update on Cyber Incident: 19 September 2024 | Synnovis

4. ***Does GSTT's Risk Register include cyber attacks on providers' networks? (Trust response)***

Yes the GSTT risk register includes a risk relating to cyber security related matters.

5. ***Does the Contract Management Group in GSTT monitor the robustness of Synnovis' IT system? (Trust response)***

The contract management arrangements associated with the contract cover a full range of pathology outputs and focus on delivery of pathology testing outputs. This includes a detailed specification of all aspects of pathology provision including relevant IT system requirements. Synnovis provides services which must be compliant with this specification.

6. ***Was Synnovis' proposed IT system in anyway downgraded during the acknowledged struggle to pull together a feasible Final Business Case for Synnovis' contract bid? (Trust response)***

No there were no down grades to the proposed IT system, in fact enhancements were made to align with the Trust's new EPR systems.

7. ***Within the terms of its contract, will Synnovis be subject to financial penalties proportionate to the costs of the attack to the SEL NHS system? (Trust response)***



**1 This document contains responses and statements provided by multiple parties. The Trusts have contributed solely to responses numbered 2, 4, 5,6,7,8,9 and 10, and have not verified and bear no responsibility for the viewpoints expressed by other parties in other responses*

The terms of the contract cover a variety of clinical, service and IT obligations. The costs of and ultimate responsibility for the attack remains under investigation, so it is too early to comment on the contractual position.

8. ***Was/Is the Synnovis cyber system more vulnerable to attack than that of the commissioning organisation****? (Trust response)*

   It is not possible to reliably answer this question without a full analysis and comparison of the respective systems.

9. ***Was there an option for Synnovis to use the IT Network of the commissioning organisation and contribute to its cost? (Trust response)***

   *No such option to make use of such infrastructure was considered.*

10. ***Will the extent of the damage to patients, hospitals and primary care be quantifiable and costed and eventually made public? (Trust response)***

    The cyber incident is still under detailed forensic examination to determine the damage that has been caused to all stakeholders. Until the damage has been fully assessed it is not possible to determine how this will be quantified and reported.



**1 This document contains responses and statements provided by multiple parties. The Trusts have contributed solely to responses numbered 2, 4, 5,6,7,8,9 and 10, and have not verified and bear no responsibility for the viewpoints expressed by other parties in other responses*