

Synnovis Cyber Incident - Frequently Asked Questions (FAQ)

Last updated: 05 December 2025

1. What happened?

Synnovis, a third-party pathology services provider, was the victim of a ransomware cyberattack in June 2024. On 20 June 2024, criminals published stolen files online. Synnovis has since completed a highly complex forensic review and begun contacting impacted organisations so they can assess their own position and take any required steps.

2. How does this affect Gateshead Health patients?

For Gateshead Health, our review indicates that **1,037 individuals** are within the dataset provided to us by Synnovis. We have assessed the contents and potential risk to those individuals as set out below.

3. What type of data is involved?

The dataset provided to Gateshead Health consists of basic identifiers (such as name, date of birth and an NHS or patient identifier) and limited health information in the form of a test name or code. It does not include test results or contact details.

4. Is this special category (health) data?

Yes. Any information about health is special category data under UK data protection law. In this case, it is limited and non-diagnostic (a test name/code only, not clinical results).

5. How identifiable is the data?

The material we reviewed is unstructured, incomplete and fragmented. On its own, it is difficult to use to directly identify an individual without additional information not contained in the dataset.

6. What is the risk to affected individuals?

Our risk assessment concluded that the likelihood of harm is minimal. We have no local evidence of misuse, targeted scams, or clinical safety impact arising from this dataset. We will continue to monitor.

7. What actions have been taken?

- Synnovis has investigated and is contacting organisations whose data was affected. They have also taken legal steps to restrict further use/publication of the stolen data and worked with national bodies on the response.
- Gateshead Health implemented immediate containment measures, strengthened controls, and ceased using the supplier for test processing where there was an alternative referral laboratory.

8. Will patients be contacted?

Under UK data protection law, each organisation must assess the risk to individuals. At this time, based on our risk assessment, the threshold for notifying individuals is not met. If further analysis indicates a higher risk to any person, we will contact them directly.

9. Do I need to do anything?

We do not believe any action is required from patients at this time. If you notice anything that concerns you, please contact our Information Governance team for advice.

- Contact us: Gateshead Health Information Governance Team – ghnt.ig.team@nhs.net

10. Where can I find more information?

- [Synnovis – Cyber Attack Information Centre](#)
- [NHS England – Synnovis cyber incident](#)
- Contact us: Gateshead Health Information Governance Team – ghnt.ig.team@nhs.net