# Tragic death linked to Qilin ransomware attack disrupts NHS pathology services in London



A tragic death in London has been officially linked to a cyberattack orchestrated by the Qilin ransomware group, which targeted Synnovis, a key pathology service provider for the NHS. The attack in June 2024 severely disrupted diagnostic services across several major hospitals in southeast London, including King’s College Hospital, Guy’s and St Thomas’, and Lewisham and Greenwich hospitals. This disruption delayed critical blood test results, contributing to the death of a patient at King’s College Hospital, marking one of the first confirmed fatalities in the UK attributed to a cyberattack on healthcare systems.

King’s College Hospital NHS Foundation Trust confirmed that a detailed review found multiple factors contributed to the patient’s death, with prolonged waits for blood test results during the incident being a significant cause. Synnovis’ CEO, Mark Dollar, expressed deep sadness over the outcome and extended sympathies to the family affected. Government officials and cybersecurity experts have highlighted the profound risks these cyberattacks pose to patient safety, with calls for independent inquiries into NHS digital security to uncover possible unreported consequences.

The attack, attributed to the Russian-speaking Qilin gang, inflicted widespread chaos over London’s healthcare network. It halted blood testing services across NHS trusts and GP practices, delaying or cancelling thousands of outpatient appointments and over 1,700 operations. Cancer treatments were also affected, with reports indicating about 1,100 treatments postponed. The disruption extended to blood transfusion services, forcing hospitals to use universal O-type blood, exacerbating a national shortage of O-type supplies. Nearly 600 patient safety incidents were logged in connection with the cyberattack, with at least two classified as severe, involving life-threatening delays or permanent harm.

Beyond operational disruption, the attackers stole and publicly released nearly 400GB of sensitive patient data on darknet platforms and messaging apps. The leaked information included personal details such as patient names, dates of birth, NHS numbers, financial arrangements between hospitals and Synnovis, and descriptions of blood tests. This represents one of the largest data breaches the NHS has faced in recent years. The National Crime Agency and National Cyber Security Centre are involved in ongoing investigations to verify the authenticity and extent of the leaked data.

The financial impact on Synnovis has been catastrophic. The cost of managing the attack and its aftermath is estimated at over £32 million, seven times higher than the company’s prior annual profits. Synnovis is a public-private partnership between the pathology firm Synlab and the hospital trusts affected and is gradually progressing through a phased recovery plan. The incident may also result in regulatory penalties from data protection authorities.

This UK incident is reminiscent of previous fatal cyberattacks on healthcare facilities internationally. Notably, a 2020 ransomware attack on the University Hospital Düsseldorf in Germany similarly caused system failures that led to the death of an emergency patient, emphasising the grave human consequences of healthcare cyber vulnerabilities. Investigators in that case found the attackers had targeted the wrong institution and provided a decryption key upon learning their mistake, underlining how lapses in cybersecurity can have irreversible effects on patient outcomes.

The Qilin ransomware gang is known for leasing its malware to affiliates and targeting critical, high-stakes sectors such as healthcare. Their operations are believed to be based in regions beyond the reach of Western law enforcement, complicating efforts to bring perpetrators to justice. The NHS and its partners face growing challenges in securing increasingly digitalised health infrastructure, where reliance on private providers and interconnected systems heightens exposure to cyber threats. Experts warn that without robust, timely cybersecurity measures, patient safety will continue to be jeopardised by such attacks.

In sum, the Qilin ransomware attack has exposed critical vulnerabilities within the NHS pathology services, with devastating effects on patient care and safety. The tragic death linked to this incident marks a somber milestone in the evolving threat posed by cybercrime to healthcare, underscoring urgent calls for enhanced security protocols and more thorough investigations to prevent further loss of life.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[3]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/), [[2]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4)
* Paragraph 2 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[2]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4), [[3]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/)
* Paragraph 3 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[4]](https://apnews.com/article/cdf59beb5b36a8eedd1470732e10ac8c), [[2]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4)
* Paragraph 4 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[6]](https://apnews.com/article/britain-nhs-ransomware-attack-qilin-2dfa0d0426ce640e5a3782900b9596f9), [[7]](https://www.theguardian.com/society/article/2024/jun/21/records-on-300m-patient-interactions-with-nhs-stolen-in-russian-hack)
* Paragraph 5 – [[5]](https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f), [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/)
* Paragraph 6 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[7]](https://www.theguardian.com/society/article/2024/jun/21/records-on-300m-patient-interactions-with-nhs-stolen-in-russian-hack), [[3]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/)
* Paragraph 7 – [[4]](https://apnews.com/article/cdf59beb5b36a8eedd1470732e10ac8c), [[7]](https://www.theguardian.com/society/article/2024/jun/21/records-on-300m-patient-interactions-with-nhs-stolen-in-russian-hack), [[2]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4)
* Paragraph 8 – [[1]](https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/), [[2]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4), [[3]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/), [[4]](https://apnews.com/article/cdf59beb5b36a8eedd1470732e10ac8c)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://hackread.com/qilin-ransomware-attack-nhs-causes-patient-death-uk/> - Please view link - unable to able to access data
2. <https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4> - A cyberattack on the NHS in June 2024, attributed to the Russian-speaking group Qilin, led to the death of a patient due to delayed blood test results. The attack targeted Synnovis, a pathology service provider for NHS hospitals, causing significant disruption at King's College Hospital and Guy's and St Thomas' NHS Foundation Trust. Qilin released 400GB of stolen data, and the breach resulted in 170 reported incidents of patient harm, mostly categorized as 'low harm.' However, one patient's death has now been officially linked to the attack. Mark Dollar, Synnovis' CEO, and a government spokesperson both expressed condolences, highlighting the profound risks such cyberattacks pose. Cybersecurity expert Dr. Saif Abed suggested that other deaths may have gone unreported due to insufficient investigations, calling for an independent inquiry into NHS digital security. This incident underscores the increasing vulnerabilities in healthcare infrastructure as reliance on private providers and digital systems grows. An ongoing law enforcement investigation is examining the full extent of the attack and its consequences.
3. <https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/> - British health officials have confirmed that a cyberattack on diagnostic services provider Synnovis in June 2024 contributed to the death of a patient at King’s College Hospital in London. The attack, linked to the Qilin ransomware gang, disrupted the UK healthcare network, causing prolonged wait times for medical test results that factored into the patient's death. Synnovis' CEO expressed deep sorrow over the incident. The perpetrators reportedly demanded a $50 million ransom, which Synnovis did not pay, leading to stolen data being posted on the dark web. The cyberattack generated over £32 million ($43 million) in damages and hindered operations at several major London hospitals. Medical service providers are frequent targets of ransomware due to the critical nature of their operations. This case marks one of the first confirmed instances of a patient death associated with a hacking incident in the UK. Similar attacks in the past have been linked to fatalities in Alabama in 2019 and Germany in 2020.
4. <https://apnews.com/article/cdf59beb5b36a8eedd1470732e10ac8c> - A ransomware attack believed to be executed by the Russian cyber gang Qilin has disrupted several hospitals in London, causing operations and appointments to be canceled. The group targeted Synnovis, a pathology lab service provider for the National Health Service, leading to significant disruptions in services, particularly blood transfusions. The incident, labeled as a 'critical' and 'major impact' event, particularly affected King's College and Guy's and St Thomas' hospital trusts. This type of ransomware attack paralyzed computer systems, severely hindering operations within the healthcare trust. Synnovis is still working to understand the attack, which was reported to the police. Ransomware, a costliest and disruptive form of cybercrime, is often difficult to combat as many gangs operate from former Soviet states, beyond Western legal reach. Qilin leases its malware to affiliates, having listed over 100 victims, according to a cyber threat intelligence company.
5. <https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f> - The cost of a ransomware attack against the laboratory services provider Synnovis in 2024 exceeded more than seven times the company's most recent annual profits. The attack, which took place in June 2024, generated estimated costs of £32.7 million, compared to profits of £4.3 million in 2023. This incident caused one of the largest patient data breaches in the NHS in recent times and led to cancellations or delays in thousands of operations and appointments at various NHS hospitals and clinics in London. The Russian cyberattack group Qilin claimed responsibility, releasing 400 GB of stolen information. Synnovis has been working slowly to restore its systems, having recently completed the 'first phase' of its recovery plan. The company expects to return to profitability thanks to a long-term outsourcing contract. Synnovis is a public-private partnership between Synlab and the trusts of Guy's and St Thomas' and King's College Hospital NHS. The ongoing investigation could still result in fines from the Information Commissioner's Office.
6. <https://apnews.com/article/britain-nhs-ransomware-attack-qilin-2dfa0d0426ce640e5a3782900b9596f9> - According to the BBC, Qilin shared almost 400GB of data, including patient names, dates of birth and descriptions of blood tests, on their darknet site and Telegram channel. 'The National Crime Agency and National Cyber Security Centre are working to verify the data included in the published files as quickly as possible,' NHS England said in a statement. 'These files are not simple uploads and so investigations of this nature are highly complex and can take weeks if not longer to complete.'
7. <https://www.theguardian.com/society/article/2024/jun/21/records-on-300m-patient-interactions-with-nhs-stolen-in-russian-hack> - It is unclear at this stage if the hack involves only hospitals in the trusts or is more widespread. The NHS’s anxiety about the impact of the attack increased on Friday after Qilin acted overnight on a threat to put stolen NHS data into the public domain, an indication that Synnovis has refused to pay a reported $50m (£40m) ransom. It is as yet unclear exactly what data, or how much of the haul, the ransomware group has made public. But the stolen data includes details of the results of blood tests conducted on patients having many types of surgery, including organ transplants; on those suspected of having a sexually transmitted infection; and on those who had had a blood transfusion. In a development that will cause anxiety among patients who have received private healthcare in recent years, Qilin’s haul is understood to include records of tests that people have had at multiple private healthcare providers. It is not clear which private healthcare firms Synnovis – a joint venture between the pathology firm Synlab and two major London acute hospital trusts – works for. The number of test results in the data that Qilin seized in the hack on 3 June is so huge because it covers tests that patients have had going back a significant number of years, sources say. The ransomware group posted 104 files of data overnight on a messaging platform. The Guardian was unable to verify the contents of the posted files, which contained a total of about 380GB of data. The post was topped with an image of the Synnovis logo, a description of the company and a link to its website. The BBC reported that the files contained patient names, dates of birth, NHS numbers and descriptions of tests. Typically, if a ransomware gang posts data it has stolen it is a sign that the victim has declined to pay a ransom to decrypt its IT systems and delete the stolen data.