# Ransomware attack on Synnovis linked to patient death and £32.7 million NHS disruption



In June 2024, a devastating ransomware attack targeted Synnovis, a London-based pathology service provider closely linked to the UK’s National Health Service (NHS). This cyber incident, attributed to the Russian-speaking criminal group Qilin, resulted in severe disruptions across several major London hospitals, including King’s College Hospital and Guy’s and St Thomas’ NHS Foundation Trust. The breach had dire consequences, contributing directly to the death of a patient due to prolonged delays in critical blood test results. This marks one of the first publicly confirmed cases in the UK where a cyberattack on healthcare infrastructure has been linked to loss of life.

The attack severely paralyzed Synnovis’ IT systems, forcing the cancellation of roughly 800 planned operations and 700 outpatient appointments. Blood transfusions and other urgent medical services were particularly impacted, with some hospitals resorting to handwritten records and asking staff for blood donations to manage supply shortages. The disruption stretched across the NHS network in London, costing an estimated £32.7 million in damages, far exceeding Synnovis’ recent annual profits and underscoring the high financial stakes involved in such breaches.

Qilin’s attack exploited an alleged zero-day vulnerability to infiltrate Synnovis’ systems, although this claim has not been independently verified. The ransomware gang demanded a staggering ransom of $50 million, an unusually large sum even by cyber extortion standards. Experts suggest this figure might have been partly aimed at raising Qilin’s notoriety in the cybercrime community. Synnovis reportedly refused or was unable to pay the ransom, prompting the attackers to publish 400GB of stolen data online. This breach compromised sensitive patient data, including names, dates of birth, NHS numbers, and blood test results, raising serious privacy concerns alongside operational chaos.

In the wake of the attack, King’s College Hospital NHS Foundation Trust conducted a thorough investigation into patient care during the incident. The patient safety review identified delays in obtaining blood test results as a contributing factor in the death of one individual. Trust representatives have engaged with the patient’s family, sharing the investigation findings and expressing condolences. Similarly, Synnovis’ CEO publicly expressed deep sorrow over the incident, while a government spokesperson highlighted the broader vulnerabilities facing healthcare infrastructure as digital dependency grows.

Cybersecurity experts have warned that this may not be an isolated tragedy. Dr Saif Abed, a specialist in healthcare cybersecurity, suggested other deaths might have gone unreported due to limited investigations into the full impacts of cyberattacks on the NHS. Calls are mounting for an independent inquiry to assess the scale and systemic risks posed by such breaches. The incident also drew attention to the continuing threats posed by ransomware groups who specifically target critical services like healthcare, confident that these organisations are more likely to refuse payment or face immense pressure to do so, all while risking patient safety.

The UK government’s ban on ransomware payments by public organisations remains a pivotal policy aiming to deter attacks, yet the severe operational disruptions and the tragic loss of life stemming from this case underscore the ongoing challenges in protecting vital public services. Meanwhile, Synnovis continues its recovery efforts, having completed the initial phase of system restoration, though the investigation by law enforcement and regulatory bodies such as the Information Commissioner’s Office remains ongoing.

This attack is part of a disturbing global pattern, with other ransomware incidents linked to patient harm or deaths in different countries, such as the United States and Germany. It highlights the critical need for robust cybersecurity measures and preparedness within the healthcare sector—not only to safeguard data but to ensure patient lives are not imperilled by digital threats.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/pro/security/ransomware-disruptions-contributed-to-a-patient-death-nhs-finds), [[2]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/), [[3]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4)
* Paragraph 2 – [[1]](https://www.techradar.com/pro/security/ransomware-disruptions-contributed-to-a-patient-death-nhs-finds), [[5]](https://apnews.com/article/23b324fd31cdebbdd57f46a0e0333a77), [[6]](https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f)
* Paragraph 3 – [[4]](https://www.bankinfosecurity.com/uk-pathology-lab-ransomware-attackers-demanded-50-million-a-25559), [[7]](https://www.insurancejournal.com/news/international/2024/06/19/780239.htm)
* Paragraph 4 – [[1]](https://www.techradar.com/pro/security/ransomware-disruptions-contributed-to-a-patient-death-nhs-finds), [[2]](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/), [[3]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4)
* Paragraph 5 – [[3]](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4), [[7]](https://www.insurancejournal.com/news/international/2024/06/19/780239.htm)
* Paragraph 6 – [[1]](https://www.techradar.com/pro/security/ransomware-disruptions-contributed-to-a-patient-death-nhs-finds), [[4]](https://www.bankinfosecurity.com/uk-pathology-lab-ransomware-attackers-demanded-50-million-a-25559), [[6]](https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f)

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

## Bibliography

1. <https://www.techradar.com/pro/security/ransomware-disruptions-contributed-to-a-patient-death-nhs-finds> - Please view link - unable to able to access data
2. <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. ([reuters.com](https://www.reuters.com/business/healthcare-pharmaceuticals/uk-health-officials-say-patients-death-partially-down-cyberattack-2025-06-26/?utm_source=openai))
3. <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. ([ft.com](https://www.ft.com/content/773c031b-a4e9-4120-bea6-d3d4c3eecdc4?utm_source=openai))
4. <https://www.bankinfosecurity.com/uk-pathology-lab-ransomware-attackers-demanded-50-million-a-25559> - Qilin also claimed that they exploited a zero-day vulnerability to gain access to Synnovis' systems. That claim couldn't be verified. Synnovis is a pathology company founded in 2009 and formerly known as Viapath. It functions as a partnership between Guy's and St Thomas' National Health Service Foundation Trust and King's College Hospitals NHS Trust in London and Munich-based medical diagnostics provider Synlab. As of Wednesday morning, Qilin's Tor-based data leak site didn't list the company as a victim or include any samples of supposedly stolen data. "Synnovis is aware of reports that an unauthorized third party has claimed responsibility for this recent cyberattack," a spokesperson told Information Security Media Group. "Our investigation into the incident remains ongoing, including assessing the validity of the third party's claims and the nature and scope of the data that may be impacted." Cybersecurity expert Brian Honan of BH Consulting said the ransom demand issued by the extortionists is "extraordinarily and unusually high," especially compared to the 2021 attack against the Irish Health Service Executive, "which took down the entire IT infrastructure for Ireland's health service" and featured a $21 million ransom demand. "Normally, ransomware demands are at a level that the criminals know the victim organization can pay," said Honan, the CEO of Dublin-based BH Consulting. "This demand for $50 million could simply be a publicity stunt by the criminals in order to raise their notoriety amongst future victims as they know by demanding this high extortion fee they will get a lot of media attention, particularly in mainstream media outlets." As the company appears to have not paid - experts urge victims to not pay whenever possible - the attackers have begun to do what they typically do next: publicly name and shame the victim, threaten to leak data they claim to have stolen during the attack, and hype their brand. ([bankinfosecurity.com](https://www.bankinfosecurity.com/uk-pathology-lab-ransomware-attackers-demanded-50-million-a-25559?utm_source=openai))
5. <https://apnews.com/article/23b324fd31cdebbdd57f46a0e0333a77> - A cyberattack on Synnovis, a company providing pathology laboratory services, forced several London hospitals to cancel operations and appointments and send patients away. The ransomware attack affected all Synnovis IT systems, causing significant service interruptions, with blood transfusions particularly impacted. The National Health Service (NHS) reported a substantial impact on King's College and Guy's and St Thomas' hospital trusts in south London. NHS England's London region is working with the National Cyber Security Centre and their cyber operations team to assess and address the incident's effects. Ransomware attacks, which involve malware to paralyze systems and demand ransom, are a major cybercrime, previously impacting Britain's health system in a 2017 attack. ([apnews.com](https://apnews.com/article/23b324fd31cdebbdd57f46a0e0333a77?utm_source=openai))
6. <https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f> - El costo de un ataque de ransomware contra el proveedor de servicios de laboratorio Synnovis en 2024 superó más de siete veces las ganancias anuales más recientes de la compañía. El ataque, que tuvo lugar en junio de 2024, generó costos estimados en 32,7 millones de libras, comparado con las ganancias de 4,3 millones de libras en 2023. Este incidente causó una de las mayores brechas de datos de pacientes del NHS en tiempos recientes, y provocó cancelaciones o retrasos en miles de operaciones y citas en varios hospitales y clínicas del NHS en Londres. El grupo de ciberataque ruso Qilin se atribuyó la responsabilidad, liberando 400 GB de información robada. Synnovis ha estado trabajando lentamente en la restauración de sus sistemas, habiendo completado recientemente la "primera fase" de su plan de recuperación. La empresa espera volver a ser rentable gracias a un contrato de externalización a largo plazo. Synnovis es una asociación público-privada entre Synlab y los trusts Guy's and St Thomas' y King's College Hospital NHS. La investigación en curso aún podría resultar en multas por parte del Information Commissioner's Office. ([ft.com](https://www.ft.com/content/d2be7c65-bf44-4a7d-9791-6deafe66659f?utm_source=openai))
7. <https://www.insurancejournal.com/news/international/2024/06/19/780239.htm> - Medical organizations swept up in the breach were aware of cyber vulnerabilities dating back for years. The incident has reverberated across the health system. In the first week, doctors canceled roughly 800 planned operations and 700 outpatient appointments, postponed blood tests and resorted to handwritten records, according to the National Health Service. At least one hospital has asked workers for blood donations to address supply shortages, while some patients needing critical care have been diverted to other facilities. Cancer treatments and C-section births were also rescheduled. The disruption has continued as the company has worked to recover its damaged computers. A Qilin website where the group listed its alleged victims disappeared from the internet in the days after the hack, though another page remains online. Synnovis wasn’t listed on that site. Responding to questions about the breach through a messaging account long associated with the gang, a representative for the hackers said that they were very sorry for the people who suffered, but refused to accept responsibility for the human cost. They suggested the attack was justified because it was in retaliation for the British government’s involvement in unspecified wars. The representative added that they had ceased contact with Synnovis after apparently failing to receive any ransom payment following the expiration of a 120-hour deadline. They said hackers had exploited an undisclosed security vulnerability – known as a “zero day” – to gain access to Synnovis’ computers. Bloomberg News couldn’t independently verify the claims about such a vulnerability. Qilin has been active since mid-2022 and has targeted more than 100 companies in more than a dozen countries, according to a list of alleged victims the gang has published on its website. The group uses ransomware to encrypt files on infected computers so that they cannot be accessed. It also often steals data from its victims, then threatens to publish the data online unless a payment is made. ([insurancejournal.com](https://www.insurancejournal.com/news/international/2024/06/19/780239.htm?utm_source=openai))