SEALD HEALTHCARE

Security = Patient Safety

When a vendor gets breached, patients pay the price.

A Patient Is Dead

In June 2024, a ransomware attack hit Synnovis, a third-party blood-testing contractor for the NHS. The breach delayed a blood test result. A patient at King's College Hospital died. This was not a failure of intent. It was a failure of enforcement.

It did not happen because the hospital was careless. It happened because a vendor was breached, and no one had technological control over what happened next.

4%

of healthcare leaders are highly confident their vendor risk assessments align with actual risk

Fortified Health Security, 2026 Horizon Report

$10.22M

average U.S. data breach cost, the highest of any country globally

IBM Cost of a Data Breach Report, 2025

80%+

of stolen health records came from third-party vendors, not hospitals

American Hospital Association, 2025

The Real Problem Is Not Hackers

Most healthcare organizations have solid perimeter security. But once patient data leaves your walls and moves to labs, billing vendors, business associates, and cloud platforms, your controls stop.

According to the American Hospital Association, over 80% of stolen patient records in recent years were taken from third-party vendors, not hospitals. **Your vendor's breach becomes your breach.**

This is not a hypothetical. 68% of healthcare organizations experienced a material cyber incident in the past 24 months. And 71% now list strengthening third-party risk as a top-three priority.

What you rely on today:

- Vendor questionnaires and annual audits
- BAAs and contractual language
- Trust, policies, and hope

A Different Kind of Control

Seald Healthcare does not ask you to trust your vendors. We make trust irrelevant.

We encrypt patient data at the record level before it ever leaves your system. Even if a vendor is breached, the data remains unreadable, unusable, and under your control.

✓ **Least Privilege, Enforced Technologically**

Access is granted per record, per user, per purpose. Not by network location.

✓ **Persistent Control After Sharing**

Revoke access to shared data at any time, even after it has been delivered.

✓ **Third-Party Risk You Can Prove**

Demonstrate to auditors and regulators exactly who accessed what and when.

✖ **TODAY**

Perimeter-only security. Data sits in plaintext. Compliant on paper, vulnerable in practice.

✓ **WITH SEALD HEALTHCARE**

Data encrypted at the source. Zero plaintext exposure. Secure even during a breach.

See It for Yourself

Identify your highest-risk vendor relationship and let us show you what technological enforcement looks like.

charlie@sealdhealthcare.com | **615-772-7663** | **sealdhealthcare.com**

Sources: Fortified Health Security 2026 Horizon Report; IBM Cost of a Data Breach Report 2025; AHA Cybersecurity Year in Review 2025; Black Book Global Healthcare Cybersecurity Survey 2026.

Synnovis story: bbc.com/news/articles/cp3ly4v2kp2o