

The Day the Hospital Went Back to Paper

Cyber threats spare no one in healthcare. Here is what recent attacks show, and what each of us can do about it

by Radhika Bawa



On 29 September, a healthcare technology company was reportedly hit by ransomware. Attackers encrypted a large volume of patient and medical data on its platform and demanded about Rs 8.5 crore.

Cyber threats to healthcare are rising, and size offers no protection. Whether you run a small nursing home or a large multispeciality hospital, you hold the same thing attackers want: patient records that cannot be replaced. Keeping that data and the care built on it safe is a partnership. Vendors, hospitals, employees and partners each hold a part of it, and a gap in any one of them puts the rest at risk. As a technology provider, we take our share of that responsibility seriously.

The record of the last few years shows why.

It keeps happening, here and everywhere

In June 2025, two large private hospitals in Delhi were pushed back to manual OPD and inpatient workflows after attacks. For a patient waiting for a bed, how the attackers got in made no difference.

In November 2022, a premier government hospital in north India lost its primary server and its first backup to ransomware. Admissions, billing and lab reports all went manual, and more than a week later the systems were still down.

Here is the detail I keep coming back to. Another large public hospital was hit around the same time and barely noticed, because most of its work was still on paper. I am not arguing against going digital. I have spent over ten years inside operating rooms helping hospitals do exactly that. I am saying that the more a hospital depends on its systems, the more it has to plan for the day those systems disappear.

It is not only India. In April 2026, a community hospital in Massachusetts lost its records system. Chemotherapy patients were sent home, ambulances were diverted, and the hospital stayed in emergency downtime for nine days. In February 2026, a hospital in Japan was breached through a VPN device used for routine maintenance, and the number of affected patients grew from about 10,000 to about 130,000 as the investigation went on.

The two supplier stories are the most telling. In June 2024, an attack on a pathology provider serving several London hospitals led them to declare a critical incident and postpone hundreds of appointments and procedures. A supplier's outage became the hospitals' emergency. And in February 2024, attackers entered one of the largest healthcare payment processors in the United States through a remote-access portal with no multi-factor authentication, stayed inside for nine days, and then deployed ransomware.

A later survey found that 74% of nearly 1,000 US hospitals reported a direct impact on patient care, even though most were never attacked themselves.

The numbers say the trend is accelerating. Analysts who track ransomware counted 410 healthcare attacks worldwide in the first half of 2026, and attacks on Indian healthcare providers grew eightfold, from a small base. India's healthcare and pharma sector also accounted for 3.79 million detections between October 2024 and September 2025, about 14% of all detections, according to Seqrite's India Cyber Threat Report 2026. Patient records cannot be replaced after a leak. Under the Digital Personal Data Protection Act, 2023, a hospital also remains responsible for personal data when a vendor processes it on its behalf.

What these incidents have in common

Read the cases side by side and the same four weaknesses keep showing up. Each one sits with a different member of the partnership, which is why no single party can fix them alone.

Backups that were not really separate. At the north India hospital, the backup went down with the primary. A backup that sits on the same network as the system it protects is a copy, not a safety net. Hospitals and their vendors share the job of keeping backups isolated and tested.

One click. Phishing emails, unknown USB drives, shared logins and unlocked workstations are how most of these stories start. No firewall stops a trusted employee from opening an attachment. This one belongs to every person on the team, which is why training matters as much as technology.

No rehearsed plan for downtime. Hospitals that kept going had paper forms, trained staff and clear instructions. The ones that struggled were inventing procedures while patients waited. Hospital leadership owns this plan, but vendors should help write and test it.

Unguarded doors for vendors and remote access. The London lab, the Japanese VPN device and the US portal without MFA all share one lesson. Attackers do not always come through your front door. They come through a connection you forgot about, a login nobody protected, or one employee's email account. Vendors and hospitals have to close these doors together.

AI is making the timeline shorter. Automated tools can now scan software for weaknesses at scale, so the gap between a flaw being found and being exploited keeps shrinking. A system that passed a security test last year may not pass today.

Five myths I still hear in hospital meetings

"We have a firewall." A firewall protects the boundary. It does not fix a flaw in an application, a stolen password, or a malicious attachment someone opened from inside.

"Our vendor says the software is secure." Ask for evidence: a recent penetration test report, who did it, and whether the findings were fixed and re-verified. The London pathology attack is a reminder of what supplier risk looks like in practice. A good vendor will welcome the question.

"Hackers go after banks, not hospitals." Hospitals hold sensitive data and cannot afford downtime. That is exactly what makes them worth attacking.

"Passwords are IT's problem." IT sets the policy. Everyone else decides whether it works. Shared logins, default passwords on new devices and unlocked screens at nursing stations and OR consoles undo a lot of good work.

"We tested it once, so we're covered." A security test is a photograph of one day. Software gets updated, new flaws get discovered, and the photograph goes out of date.

I remember the time when we started selling OR integration systems in the country as a distributor. The password was the easiest and most well-known thing about the system. Now, of course, we know better!

What I would do this month

None of this needs a large budget. It needs a decision to start, and it works best when hospitals, staff and vendors do it together.

1. Map what touches patient data. List every application and device that stores, processes or accesses it, including the ones installed years ago that nobody owns anymore. You cannot protect what you have not listed.

2. Fix the basics on accounts. Replace default passwords, end shared logins, switch on multi-factor authentication for remote access (including the maintenance links your vendors use), and remove access the day someone leaves or changes role.

3. Ask every vendor for evidence. Four questions are enough to start. Was the software tested by a CERT-In empanelled auditor? Was the testing done in the actual deployment environment? Were the findings fixed and independently verified? Is reassessment periodic? Vulnerability assessment and penetration testing (VAPT) exist to answer exactly these. For web-based clinical applications, web application penetration testing against the OWASP Top 10 is the standard reference.

4. Prove your backups. Keep at least one copy offline or isolated from the main network, and actually restore from it on a schedule. Until you have done a restore, you do not know that you have a backup.

5. Rehearse paper mode. Print the forms. Run a drill where the system is "down" for two hours and see what breaks. Do it before the attacker does it for you.

One more habit: a short awareness session on phishing and password hygiene, repeated regularly, does more than most people expect. Staff who report an odd pop-up in the first five minutes can save a hospital five days.

Where CREA fits

1. Where OR integration fits

A lot of patient data is created in the operating room: surgical video, images and recordings. Without a system, it leaves the OR on whatever is at hand, a pen drive, a phone, a portable hard disk, and from that moment nobody can say who has a copy or where it went. There is no audit trail. OR integration fixes this at the source. It makes sure that only authorised users can access patient videos and images, and it removes the need for stray pen drives and portable devices to carry them around. A centralised archival platform then keeps everything in one place, with authentication and encryption in place, so that every access is controlled and traceable. At Esbee Dynamed, we build CREA, a digital operating room integration platform that connects surgical devices with clinical systems such as HIS and PACS using HL7 and DICOM.

2. What we have done in our own company

Because CREA sits inside the OR, we asked ourselves the same question we are asking you to put to every vendor: where is the proof? Our part of this partnership is to make our security something you can verify, not just trust.

CREA has undergone independent web application penetration testing by a CERT-In empanelled auditor, following CERT-In guidelines and the OWASP Top 10. Testing was done in the actual deployment environment. The result was a pass, with every finding independently verified as closed and zero open vulnerabilities at the time of certification. We reassess periodically, because a certificate describes one day, not every day after it.

Certification is one part of it. We have also brought a CTO on board, we are sensitising our teams on the everyday dos and don'ts of security, and we are moving towards zero trust, where no user or device is trusted by default.

We share this so that your IT and procurement teams have documented evidence to review, not just our word for it.

Security is a habit, not a certificate. The hospitals that come through an attack best are not the ones that were never targeted. They are the ones that planned for it, together with their staff and their vendors. Whether you run a small nursing home or a large multispeciality hospital, we would like to be part of that plan.

See secure OR integration in action. Visit Esbee Hive, our experience centre in Mumbai, to see CREA in a live operating room setup and go through its security documentation with our team. [Book a CREA walkthrough at Esbee Hive]

Esbee Dynamed specialises in OR integration and connected surgical instrument tracking solutions. To learn how we can support your operating theatre, contact our team.

Write to us at info@esbeedynamed.com for more info.