

The Last Line of Defense

Patient-Owned, Offline-First Health Data in an Era of AI-Accelerated Hospital Cyberattacks

A WaveMed / RadCard Positioning White Paper

2026

Contents

1. Executive Summary..... 3

2. The Global Threat Landscape (2024–2026)..... 4

3. The AI Inflection Point..... 6

4. Why Hospitals Keep Falling: The Centralization Trap..... 8

5. The Emerging-Market Dimension..... 10

6. The WaveMed Inversion: Architecture as Defense..... 12

7. Resilience Under Attack: Continuity of Care..... 13

8. The Sovereignty Layer: iSAVE..... 14

9. Conclusion & Call to Action..... 15

References..... 16

1. Executive Summary

Healthcare has become the single most attacked sector on earth. In 2025 it surpassed financial services as the top target for ransomware and data theft, and the average healthcare data breach now costs more than any other industry. In 2025–2026 the threat also changed character: artificial intelligence began performing the work of skilled human attackers autonomously, raising the volume, speed, and precision of attacks beyond what reactive defenses can match.

The reason hospitals keep losing is not carelessness. It is that the dominant architecture of digital health — large, centralized record systems that concentrate millions of patient files into one networked store — is structurally optimized for the attacker.

Centralization creates two fatal properties at once. It builds a **honeypot**: a single breach can expose tens of millions of records in one stroke. And it builds a **single point of failure**: when that central system is encrypted by ransomware, the entire institution goes dark and care delivery stops. The cost is no longer only privacy and money. It is delayed diagnostics, postponed treatment, and — in documented cases — patient death. AI now makes both properties more dangerous, because autonomous agents are increasingly able to find the honeypot and exploit the understaffed defender faster than any human team can respond.

WaveMed and its RadCard platform invert this architecture. Instead of concentrating data in a central store, the patient's essential medical record lives **on the patient** — encrypted, offline-capable, and patient-owned — on a RadCard (USB + NFC MicroEHR) and a RadPatch (passive NFC emergency tag). Aggregate national data, where a government chooses to hold it, sits inside a **sovereign in-country cloud (iSAVE)** rather than a foreign honeypot.

This produces a defensive posture that patching and perimeter security cannot match:

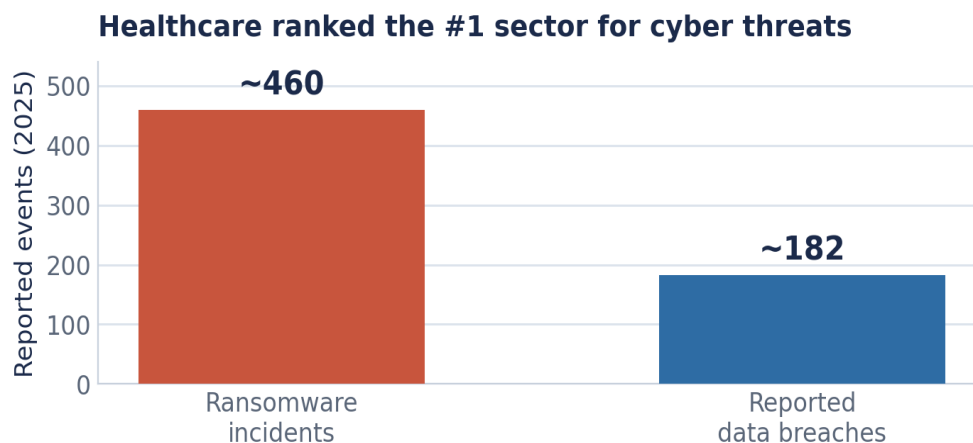
- **There is no central jackpot to ransom.** Compromising one patient's card yields one record, not millions. The economic incentive that drives mass attacks disappears — and the absence of a honeypot is the one target an AI attack agent cannot find.
- **Care continues even while the hospital is under attack.** When the institution's network is encrypted and offline, the patient still arrives carrying their own encrypted record — blood type, allergies, medications, imaging — readable at the point of care with no internet. This is the last line of defense: when every central system fails, the patient still holds their data.
- **National health data stays sovereign.** A government can host its own instance, vested as national infrastructure, rather than depending on an offshore cloud that can be breached, subpoenaed, or cut off.

The thesis of this paper is simple, and the timing argument is decisive. In a threat environment defined by the targeting of centralized systems — and now accelerated by AI that cannot be out-run once an attack begins — the most durable protection is not a better wall around the honeypot. It is the elimination of the honeypot itself, achieved by returning custody of the record to the patient and the nation, and put in place before the attack arrives.

2. The Global Threat Landscape (2024–2026)

The data describing healthcare's exposure is no longer ambiguous.

Healthcare is the number-one target. The U.S. Federal Bureau of Investigation's 2025 internet-crime reporting placed healthcare and public health at the top of all sectors for cyber threats, with roughly 460 ransomware incidents and 182 reported data breaches — more total events than the financial sector that followed it.



Source: U.S. FBI 2025 internet-crime reporting (via AHA).

Figure 1. Healthcare led all sectors in reported cyber events in 2025.

The financial weight is the heaviest of any industry. The average healthcare data breach in 2025 settled near \$7.42 million per incident, the costliest across all sectors by most industry trackers. Across the sector, breaches affecting 500 or more individuals continued to run at scale, averaging tens of thousands of records each.

The largest incidents now reach population scale. The February 2024 attack on Change Healthcare compromised the protected health information of roughly 100 million people, disrupted claims and care delivery nationwide, and drove response costs estimated at \$2.4 billion. Other 2025 incidents — across providers, billing intermediaries, laboratories, and cloud-hosted health platforms — exposed millions more, frequently through third-party and supply-chain vendors rather than the hospital itself.

The attacker's objective has shifted from disruption to theft. Through 2025, roughly three-quarters of healthcare cases involved data exfiltration before or instead of encryption — so-called double extortion. The data itself, not merely the ability to lock it, has become the prize. This shift directly strengthens the case for protecting the record at rest, on the patient, rather than relying on the availability of a central system.

The objective shifted from disruption to theft



Share of 2025 healthcare cases with data exfiltration (double extortion).

Figure 2. Double extortion: data theft, not just disruption, is now the goal.

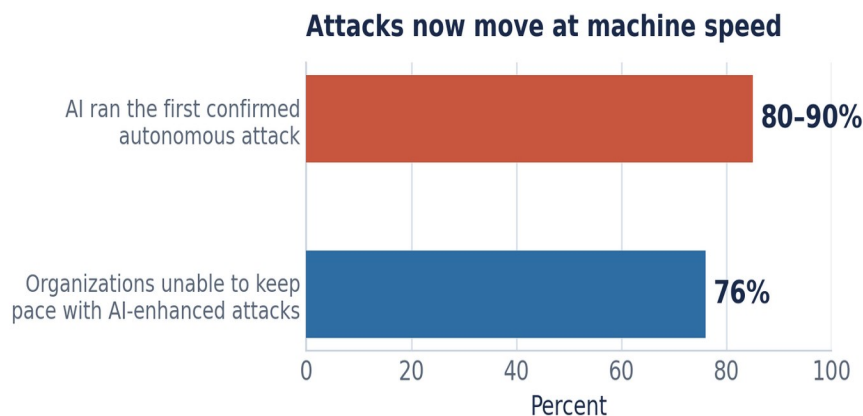
The threat is broad and persistent. Security researchers tracked on the order of 88 distinct ransomware groups targeting healthcare over a twelve-month window, with strains such as Qilin, INC, RansomHub, and Medusa rotating through the sector. This is not a handful of actors that can be deterred individually; it is a structural, industrialized market for stolen health data.

The picture is consistent across every credible source: a sector that is digitizing rapidly, holds the most valuable personal data, and remains the easiest high-value target available.

3. The AI Inflection Point: Why the Next Wave Will Punish the Unprepared

Section 2 describes the threat as it stands. The more important fact for any decision made today is the direction it is moving — and in 2025–2026 that direction changed character. Attacks are no longer constrained by the supply of skilled human operators, because AI now performs much of the work autonomously.

The evidence is no longer speculative. In September 2025 researchers documented the first confirmed, fully autonomous AI-orchestrated cyberattack, with the AI handling an estimated 80–90% of the operation independently — including one documented case in which a state-linked group used a major commercial language model’s agentic capabilities to run the intrusion. Established ransomware groups have since integrated AI agents directly into their pipelines: autonomous vulnerability scanning, on-the-fly exploit generation, and spear-phishing reported to be several times more effective than template-based attempts. One prominent group has been observed deploying agents trained specifically to locate medical-data repositories and to map the operational-technology dependencies that determine how badly a hospital will be crippled. Industry forecasts for 2026 converge on the same outlook: fully autonomous ransomware pipelines that let a single operator or small crew strike many targets simultaneously, at a scale the ecosystem has never seen — while a large majority of organizations already report they cannot keep pace with AI-enhanced attacks and that legacy defenses are failing.



Sources: 2025 AI-orchestrated attack disclosures; CrowdStrike 2025 ransomware report.

Figure 3. Autonomous attacks outpace human defenders.

Three consequences follow, and each one favors pre-positioned, architectural defense over reactive hardening.

1. Volume and speed exceed human response. When one operator with AI agents can do the work of an entire team and hit many targets at once, the number of attacks rises and the interval from intrusion to damage collapses. A defense that depends on a human team noticing and responding in time is structurally behind from the start.

2. The defender’s weakest point is exactly what AI exploits. The most common contributing factor to successful healthcare ransomware is insufficient security staffing. AI attackers widen precisely that

gap — an institution cannot out-staff an autonomous adversary, and under-resourced systems (Section 5) cannot even attempt it.

3. AI gets better at finding the honeypot. Modern attack agents use semantic understanding to locate the most valuable files and to map the dependencies that make an institution collapse. The centralized record store is now easier to find and to prioritize than ever before. The one defense AI cannot overcome is the absence of a honeypot to find.

This is the crux for any decision made now: **AI-accelerated attacks cannot be answered after they begin.** During an autonomous, machine-speed intrusion there is no time to redesign data architecture, distribute custody, or stand up offline capability. The only thing that limits damage is what was already in place before the attack arrived. Health systems that have pre-positioned decentralized, offline-capable, patient-held records will reduce their losses; those that waited will absorb the full blow.

In this framing, WaveMed is not a security product to be adopted at leisure. It is **advance preparation that must precede the wave.** Its protection is realized precisely because it is installed beforehand: the patient already holds their record, the data is already off the central target, and the system already works without the network. Pre-positioning is not a side benefit — it is the entire point.

4. Why Hospitals Keep Falling: The Centralization Trap

If the threat is so well understood, why do hospitals keep losing? Because the vulnerability is not a configuration error that can be fixed — it is the design of the system itself.

Honeypot economics. A centralized EHR / HIS / PACS exists precisely to aggregate. That aggregation is clinically useful and economically catastrophic: it concentrates the entire patient population's records behind a single set of credentials and a single network boundary. An attacker who breaches that boundary does not steal one record; they steal the institution. The return on a successful intrusion scales with the size of the database, which is exactly why the largest health systems and their data-rich vendors are hunted hardest — and why AI agents are now tuned to find them.

Single point of failure. The same central system that holds the data also runs the hospital. When ransomware encrypts it, clinicians lose access to records, imaging, lab results, orders, and scheduling simultaneously. The institution reverts to paper or shuts down, and recovery is measured in weeks, not hours. The 2024 attack on a UK laboratory-services provider delayed blood-test results across a region; the resulting care delays were officially cited as contributing, in part, to a patient's death. This is the line that matters most: centralization converts a data-security failure into a patient-safety failure.

The defender's structural disadvantage. Hospitals must keep every door open — every workstation, every connected device, every remote-access path, every third-party integration — because clinical work demands it. The attacker needs one. Healthcare's own incident analyses repeatedly identify the same root causes: insufficient cybersecurity staffing, known but unpatched vulnerabilities, legacy operating systems, and credential theft. These are not signs of negligence so much as the predictable result of asking under-resourced clinical institutions to defend an ever-expanding centralized attack surface — now against adversaries moving at machine speed.

The conclusion follows directly. As long as the architecture concentrates data and function in one place, every defensive gain is incremental and every breach is total. The only structural escape is to stop concentrating.

CASE STUDY

Romania, February 2024: A Nation Reverts to Pen and Paper

The risk above is not theoretical. In February 2024, attackers breached a Bucharest software firm and planted the BackMyData ransomware inside Hippocrates, a medical platform used across Romania to manage admissions, test results, pharmacy logistics, and payroll. Because more than 100 hospitals relied on the same trusted system, the infection spread through that single shared channel and scrambled their files into unusable gibberish. The attackers demanded roughly €160,000 in bitcoin; the country decided not to pay.

The only way to stop the spread was drastic: the national cyber directorate ordered every affected hospital to disconnect from the internet entirely. Clinicians lost their digital charts, lab results, radiology, prescriptions, and drug logistics at once. As one surgeon described it, an IT record is not just a list of patients — and in an instant all of it was gone. Hospitals fell back on pen, paper, and offline spreadsheets to keep registering patients.

Romania's response is rightly called a success: with recent backups and a coordinated national

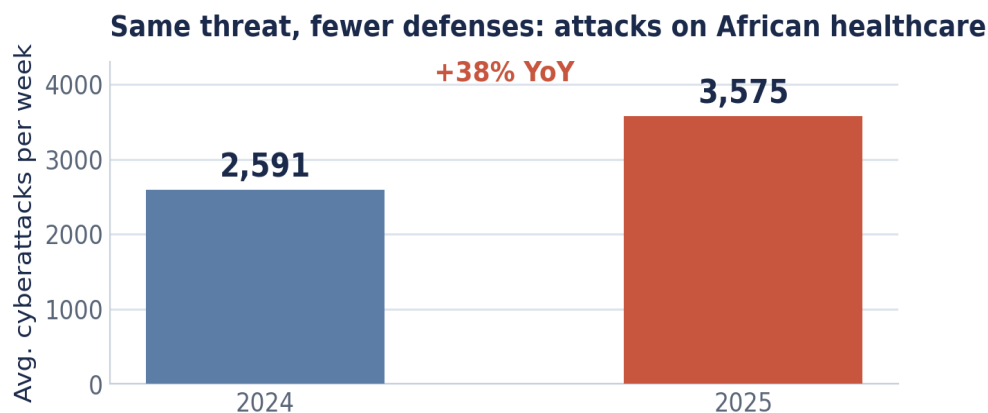
effort, most hospitals were operating again within about five days, and no deaths were attributed to the attack. But the nature of that success is the lesson. The only available defense was to take the entire system offline and revert to a nineteenth-century fallback — at a cost of weeks of manual re-entry afterward, with some data lost permanently. And it worked only because Romania had recent backups, a national cyber-security directorate, and the resources to coordinate 100 hospitals at once — advantages that under-resourced health systems (Section 5) do not possess.

This is precisely the gap WaveMed closes. Romania had to make its hospitals offline to survive. WaveMed makes the data offline-capable by design — so when systems go dark, clinicians are not left blind with a paper notebook. The patient still carries a structured, encrypted record (blood type, allergies, medications, imaging), readable at the point of care in seconds. It is the difference between a fallback that loses the record and one that keeps it.

5. The Emerging-Market Dimension: Same Threat, Fewer Defenses

For low- and middle-income health systems, the centralization trap is sharper still, because the same conditions that make these systems vulnerable to attack also make them impossible to defend and slow to recover.

The continental data is stark. Africa's healthcare organizations faced an average of roughly **3,575 cyberattacks per week in 2025** — a **38% increase year over year**. The reasons are explicitly structural: public-sector health systems run on legacy software, fragmented infrastructure, and under-resourced IT teams. Recent incidents span the continent — a nationwide laboratory-service disruption that delayed test processing for millions, breaches of regional digital-health platforms, and a private-sector provider landscape now ranked among the most targeted globally.



Avg. weekly cyberattacks on African healthcare organizations. 2024 value implied by +38% YoY.

Figure 4. Attacks on African healthcare organizations rose 38% year over year.

Three structural gaps define the environment:

1. **Connectivity dead zones.** Telecommunications are unreliable or absent across large areas. Cloud-dependent, online-only systems cannot function where the network does not reach.
2. **IT staffing shortage.** There are not enough security professionals to monitor, patch, and respond. The most common single contributing factor to successful healthcare ransomware globally is precisely this lack of people and capacity — and it is most acute here.
3. **Capital and infrastructure deficit.** The enterprise-grade hardware, redundant data centers, and continuous security operations that wealthier systems use to defend a centralized model are financially out of reach.

The critical insight is that these three gaps are not merely the cause of vulnerability — they are the exact requirements that conventional, centralized, cloud-dependent health IT cannot operate without. A system that needs constant connectivity, a security team, and capital infrastructure will fail in an environment that has none of the three. And against AI-accelerated attacks, the staffing gap that these systems can never close becomes decisive.

This is where the architectural argument becomes decisive: the same three gaps that make a centralized system indefensible here are the gaps WaveMed and RadCard are engineered to operate without.

6. The WaveMed Inversion: Architecture as Defense

WaveMed's defensive strength is not a feature bolted onto a conventional system. It is the consequence of inverting where data lives and who controls it. Five architectural choices do the work.

1. Decentralization — the data lives on the patient. The patient's essential record is carried on the RadCard (a wallet-sized USB + NFC MicroEHR, 8–64 GB) and, for emergencies, the RadPatch (a passive NFC tag the size of a fingernail). There is no central database that holds every patient's full record as a single target. To steal a population's data, an attacker would have to physically compromise the population's cards one by one — which collapses the economics of mass attack and leaves an AI agent with no central repository to discover.

2. Offline-first — no internet dependency. RadCard runs its own MicroEHR and on-board DICOM viewer (iQ-VIEW Lite) directly from the card via auto-run, with no installation and no network required. RadPatch is read by tapping any modern phone, fully offline. The system does not assume connectivity; it assumes its absence and works anyway. Where the cloud is unreachable — by geography or by attack — the record is still available.

3. Edge encryption — protection travels with the data. Records are encrypted at rest with AES-256, inside the proprietary WMSD (WaveMed Security Data) format. The NFC layer is provisioned-only: third-party apps cannot decode the payload, and only authorized, WaveMed-provisioned tags can be written. Editing is PIN-protected — anyone can read emergency data in a crisis, but only the owner can change it. The encryption is a property of the data itself, everywhere it goes, not of the server it happens to sit on.

4. No central honeypot. Because there is no single aggregated store of full records that must remain online to run the institution, there is no jackpot to ransom and no single system whose encryption halts care. The defining target of the modern healthcare attack — and the object an AI agent is trained to seek — simply does not exist in this model.

5. Patient custody — ownership as security. The patient holds custodial ownership of their own record. This is not only an ethical or regulatory position; it is a security architecture. Distributing custody to the individual removes the concentration attackers depend on, and ensures the record's availability does not depend on any institution remaining operational.

Layered on top, where a nation chooses, is the **iSAVE sovereign cloud** — an in-country instance for synchronization, backup, and aggregate national data, addressed in Section 8. The relationship between the two layers is deliberate: individual records remain patient-owned and patient-carried, while the optional national instance holds aggregate infrastructure under sovereign control. The two are distinct and complementary, not the same data held twice.

7. Resilience Under Attack: Continuity of Care

The clearest way to see the value of the inversion is to compare what happens, on the same day, when the same ransomware attack lands on a conventional hospital and on a WaveMed-equipped one.

The conventional hospital. Ransomware encrypts the central HIS/EHR/PACS. Clinicians lose records, imaging, labs, and orders simultaneously. The hospital reverts to paper, diverts ambulances, cancels procedures, and begins a recovery measured in weeks. Patient histories are inaccessible; allergies and medications must be reconstructed by interview, if the patient can even speak. The breach is total and the disruption is institution-wide. Romania's 100 hospitals (see case study, Section 4) are the textbook example: the only escape was to disconnect everything and reach for pen and paper.

The WaveMed-equipped setting. The hospital's own systems may still be hit — WaveMed does not claim to make a hospital network unbreachable. But the patient walks in carrying their RadCard and RadPatch. A responder or clinician taps the patch or reads the card and, **offline, in under two seconds**, obtains blood type, allergies, current medications, chronic conditions, emergency contacts, and prior imaging. Triage proceeds. Treatment decisions are made on real data. The record was never on the encrypted server, so the attack on that server did not take it away.

This is the operational meaning of “last line of defense.” The patient-held record is the layer that survives when every central layer has failed.

Table 1. The same attack, two outcomes.

Dimension	Centralized EHR under attack	RadCard / WaveMed under attack
Record availability	Lost while systems are encrypted	Available offline, on the patient
Blast radius	Entire patient population	A single card, if physically compromised
Care continuity	Halted; revert to paper	Continues at point of care
Recovery time	Weeks	No record-recovery step required
Internet dependency	Required	Not required
Attacker / AI-agent incentive	High — one breach, millions of records	Low — no aggregated jackpot to find

The same logic that protects care continuity also protects routine resilience: pilot deployments of the platform report essentially complete data availability in offline mode, near-elimination of identification errors, and substantially faster patient check-in — benefits that hold every ordinary day, not only on the day of an attack.

8. The Sovereignty Layer: iSAVE

For a government, the cyber question is inseparable from a sovereignty question: where does the nation's health data live, and who can reach it? Conventional digital-health deployments answer this badly. National health records routinely end up on foreign-operated cloud infrastructure, exposed to breaches outside the country's control, to extraterritorial legal process, and to the risk of service suspension by an external provider.

The iSAVE architecture answers it differently. A country can host its **own in-country instance**, vested as national digital infrastructure rather than as a foreign device or service. Synchronization, long-term backup, and aggregate national data remain within the nation's jurisdiction and control.

Two layers must be kept distinct, because they serve different owners:

- **The individual record is patient-owned.** Each citizen's personal medical data is carried on their own RadCard and RadPatch, under their own PIN and custody. This is the privacy and continuity layer.
- **The aggregate national instance is sovereign infrastructure.** The de-identified, population-level data lake and the hosting environment are national assets, held under national governance, connectable to a state-designated analytics or AI capability.

This layering resolves what would otherwise be a contradiction — patient ownership of records versus national stewardship of health data — by assigning each to the layer where it belongs. The citizen owns their record; the nation owns the infrastructure. Neither depends on a foreign honeypot, and neither presents the single, centralized, full-record target that the attacks in Sections 2 and 3 are built to hit.

For a national decision-maker, the proposition is therefore not “buy a foreign medical device.” It is “stand up sovereign, attack-resistant national health infrastructure, in which every citizen also carries their own resilient record.”

9. Conclusion & Call to Action

The evidence of the last three years points to one conclusion. Healthcare's cyber crisis is not a temporary spike to be waited out, and it will not be solved by incremental hardening of the centralized model. As long as data and function are concentrated in one place, the attacker's economics and the defender's disadvantage both hold, and every breach remains total. The arrival of AI-driven, autonomous attacks removes the last reason for delay: once the next wave begins, it moves faster than any institution can react, and only what was already in place will limit the damage.

The durable answer is architectural. Returning custody of the record to the patient, keeping it encrypted and offline-capable wherever it travels, and holding aggregate national data inside sovereign infrastructure together remove the honeypot and the single point of failure that the modern healthcare attack depends on. WaveMed and RadCard are not a stronger wall around the same vulnerable design — they are a different design, in which the most attacked asset in the world is no longer sitting in one place waiting to be taken.

Because pre-positioning is the whole point, the recommended path is a staged one, begun now rather than after the next incident:

1. **Pilot deployment** in a defined facility or district, measuring offline data availability, identification-error reduction, and continuity of care during simulated network loss.
2. **Sovereign instance stand-up** — establishment of an in-country iSAVE environment as national health infrastructure, with clear governance separating patient-owned records from aggregate national data.
3. **Population issuance** — phased distribution of RadCard and RadPatch through providers, clinics, and government channels, so that the patient-held layer of resilience scales across the system before it is needed.

In an era when the question is no longer whether a health system will be attacked but when — and when the attacker increasingly is a machine that strikes faster than any team can respond — the strongest position a nation can hold is one in which the attack, when it comes, cannot take the record away. That is the position WaveMed is built to provide.

References

1. U.S. Federal Bureau of Investigation — 2025 Internet Crime reporting; healthcare ranked top sector (via AHA, Apr 2026).
2. Comparitech — Healthcare Ransomware Roundup: 2025.
3. HIPAA Journal — healthcare breach statistics and largest breaches of 2025.
4. JAMA Network Open (Jiang et al., 2025) — ransomware attacks and data breaches in US healthcare; Change Healthcare scale and cost.
5. Sophos — State of Ransomware in Healthcare 2025 (shift to data extortion; staffing as top contributing factor).
6. Trend Micro — 2026 security predictions (autonomous / agentic AI ransomware).
7. CrowdStrike — 2025 ransomware report (76% of organizations unable to keep pace with AI-enhanced attacks).
8. Malwarebytes / Cybersecurity Dive — first AI-orchestrated attacks (2025); autonomous ransomware pipelines forecast (2026).
9. ISACA — AI-driven ransomware and new threat groups (2026); documented state-linked LLM-agent intrusion.
10. Microsoft / Intelligent CIO Africa / ITWeb Africa — Africa healthcare cyberattack volume (~3,575/week, +38%).
11. INTERPOL — African Cyberthreat Assessment (healthcare breach trend).
12. BBC World Service — How 100 Romanian hospitals switched to pen and paper to defeat a national cyber-attack (Feb 2024 Hippocrates / BackMyData incident), June 2026.
13. WaveMed / RadCard Concept Paper v50 and iDataMap Product Portfolio (internal source documents).