Prepared By: cellhub

Isolated Recovery Environments (IRE) for Healthcare

How 5G, SIM-Based Identity & Mobile SASE Create a True Cyber Sanctuary

cellhub

1. Executive Summary

Healthcare has become the #1 target for ransomware in the United States, with attacks halting clinical operations, diverting emergency rooms, shutting down imaging systems, and putting patient safety at risk. When a hospital's primary network is compromised, traditional recovery methods often reintroduce infection because the restore process relies on the same "dirty" infrastructure attackers have already infiltrated.

This is why **EPIC now recommends Isolated Recovery Environments (IRE) as a foundational cyber-resilience capability**—and we could not agree more.

This white paper explains how a modern IRE—augmented with **Private 5G**, **SIM-based identity**, and **Mobile SASE**—creates not just a backup strategy, but a **digitally and physically sterile environment** capable of restoring Electronic Health Records (EHR), PACS systems, and critical Tier-0 applications safely and rapidly.

This is the first industry reference architecture that shows how **5G slicing**, **Zero-Trust device identity**, and **campus-wide signal propagation through DAS** elevate the IRE from an IT project to a **clinical continuity system**.

---

2. The Problem: Healthcare Recovery Happens on Compromised Networks

During a cyberattack, the hospital network itself becomes untrusted:

- Lateral movement corrupts backups.
- Credential theft compromises domain controllers and VPNs.
- IT teams attempt restores into networks still harboring active malware.
- Recovery rooms themselves can be reinfected when connected to LAN/Wi-Fi.

This creates a paradox:

How do you safely restore clinical systems when the recovery infrastructure is itself unsafe?

Traditional "clean rooms" plugged into the same core as the infected network do **not** provide isolation. Hospitals need a recovery environment that attackers *physically cannot reach*—even if they control the LAN, Wi-Fi, or internet pathways.

---

3. The IRE Solution: A Dedicated, Air-Gapped Cyber Sanctuary

An **Isolated Recovery Environment (IRE)** is a digitally sterile "clean room" that:

- Operates on **independent carrier-grade spectrum** attackers cannot access.
- Authenticates devices using **SIM hardware identity**—not software credentials.
- Enforces Zero Trust boundaries through **Mobile SASE** before any packet enters.
- Uses **5G slicing** to accelerate forensics and data restoration in parallel.
- Extends secure access across the hospital through **5G DAS coverage**.

This creates a safe space to:

- Boot virtual machines for forensic analysis
- Restore Tier-0 systems from immutable storage
- Validate clean backups
- Bring clinicians back online through gated re-entry

EPIC's framework recognizes IRE as essential because it eliminates the risk of reinfection during recovery—**the highest-risk phase of a ransomware event**.

---

4. Architectural Foundations of a Modern IRE

4.1 Private 5G: The Independent Transport Layer

Private 5G provides **true physical and logical air-gap isolation** by operating on dedicated licensed spectrum separate from:

- Hospital LAN
- Hospital Wi-Fi
- Public internet

- Any compromised infrastructure

Benefits:

- Attackers cannot reach the IRE core—there is no IP path.
- Only authorized SIM provisioned devices can attach to the network.
- No shared credentials or VPNs, eliminating the most common compromise vectors.

4.2 SIM-Based Identity: Hardware-Locked Access

In the IRE design:

- The SIM **is the credential**.
- Identity cannot be spoofed, phished, or replayed.
- Devices without approved SIMs cannot physically connect to the IRE slice.

This prevents:

- Rogue device connections
- Session hijacks
- Unauthorized lateral movement

4.3 Mobile SASE: Zero-Trust Boundary at the Edge

Before any traffic enters the IRE, SASE enforces policies:

- ZTNA gating
- Threat inspection
- Application-level controls
- URL filtering
- Microsegmentation

This ensures the IRE stays clean even during active recovery operations.

---

5. The 5G Slicing Breakthrough for Recovery Speed

Restoring a hospital after a ransomware attack is a race against:

- ER diversion
- Patient safety events

- Financial penalties
- Reputational damage

5G network slicing **separates recovery workloads into dedicated lanes**, preventing congestion and dramatically accelerating MTTR.

Recovery Workflow Enhanced by Slicing

Phase	Activity	Slice	Benefit
Phase 1: Forensics	Boot VMs in isolated sandbox	URLLC Slice	Real-time diagnostics, instant behavioral analysis
Phase 2: Mass Data Restore	Move Tier-0 EHR from immutable storage	eMBB Slice	High-throughput server-to-server restores
Phase 3: Clinical Re-Entry	Bring clinicians back online	ZTNA/SIM slice	Validated, controlled return to operations

Outcome:

Forensics and restore processes run in parallel, not in competition.

This is the first time recovery workflows have deterministic bandwidth.

---

6. IRE Everywhere: Campus-Wide Coverage via 5G DAS

Hospitals cannot transport infected machines to a central recovery room during an attack. A scalable IRE must extend to:

- Patient rooms
- Operating rooms
- Radiology departments
- Sub-basements
- Offsite clinics

5G Distributed Antenna Systems (DAS) extend the IRE's isolated signal everywhere recovery teams need to work.

Benefits:

- **Forensics at the bedside**
- **Persistent secure sessions across floors**
- **Bypasses compromised hospital LAN/Wi-Fi entirely**

The entire hospital becomes a potential recovery zone.

---

7. Deployment Model: Carrier + SASE + Integrator

A modern IRE is not a single product—it is a **three-layer engineering system**:

T-Mobile (Network Layer)

- Dedicated isolated spectrum
- Private 5G core and slicing
- Air-gapped transport layer

SASE Provider (Security Layer)

- Zero Trust enforcement
- Traffic inspection
- SIM validation
- Clean Room policy application

Cellhub + (Integrator Layer)

- RF validation
- Break-glass workflow engineering
- DAS coverage design
- Operational readiness testing

This tri-party alignment ensures the IRE is not theoretical—it works in the real operational constraints of an active hospital.

---

8. Business Case: Why Hospitals Must Invest in IRE

Cost Drivers & ROI

Factor	Reason	Outcome
Targeted CAPEX	Air-gapped 5G core, recovery SIMs, architecture validation	Guarantees sterile environment
Infrastructure leverage	Use existing DAS fiber + logical slicing	Saves millions vs. "shadow networks"
5–7 month readiness	Golden image creation, kill-switch testing	Ensures confident real-world activation
Downtime avoidance	Healthcare outages cost $1M+ per hour	Faster return to clinical operations

Strategic Value Drivers

- **Avoids ransom payments**
- **Reduces cyber insurance premiums**
- **Prevents ER diversion and patient safety events**
- **Provides defensible evidence for HIPAA and NIST resilience audits**

The IRE becomes the hospital's **digital life support system**—the only environment trusted during cyber crisis.

---

9. Governance: Ensuring IRE Readiness 365 Days a Year

A clean room that works only "on paper" is not resilience. Governance ensures constant readiness.

Required Activities

- **SIM-based air-gap enforcement**
- **Quarterly clean-restore simulations**
- **Immutable chain-of-custody logging**
- **Continuous monitoring of RF and SASE health**

A sample dashboard (from the deck) includes:

- 15 authorized agents
- Last drill: 14 days ago (success)
- Air gap integrity: 100%

- Compliance score: 98/100

This creates operational confidence before crisis strikes.

---

10. Conclusion: IRE Is Now Essential Healthcare Infrastructure

The industry consensus—reinforced by EPIC's recommendation—is clear:

Every hospital needs an Isolated Recovery Environment.
And every IRE needs dedicated 5G, SIM identity, and Mobile SASE to be truly sterile.

As ransomware sophistication grows, only architectures built with **independent transport**, **hardware identity**, and **Zero Trust at the edge** can guarantee safe restoration of clinical systems.

This white paper, together with the companion **Reference Architecture Deck**, provides healthcare leaders, CISOs, and CTOs with the engineering blueprint to build a functional cyber sanctuary that restores operations faster and protects patient safety when it matters most.

Link to companion Reference Architecture Deck