DATA SHEET

CloudWave Epic IRE Assessment

Cyber Recovery Readiness for Epic Environments

THE CHALLENGE

Healthcare organizations are facing sustained ransomware pressure, and Epic downtime has rapidly shifted from an IT inconvenience to a clinical safety risk. Traditional disaster recovery strategies were not designed for modern cyber events where identity systems, administrative access, and trusted infrastructure may be compromised simultaneously.

Many organizations believe they can "restore Epic," but have never validated whether that recovery is **clean**, **isolated**, or **operationally executable** under attack conditions. Backup success does not guarantee recoverability, and recovery timelines often depend on undocumented dependencies such as identity services, interfaces, certificates, and administrative access paths.

At the same time, regulatory expectations are tightening. Proposed updates to the HIPAA Security Rule introduce explicit expectations for documented 72-hour restoration procedures, criticality analysis, backup recency, and repeatable testing evidence. For Epic environments, this raises a fundamental question:

Q: Can Epic be restored safely, quickly, and predictably during a cyber event, not just a traditional outage?

Traditional disaster recovery strategies were not designed for modern cyber events where identity systems, administrative access, and trusted infrastructure may be compromised simultaneously.

CLOUDWAVE'S SOLUTION

The **CloudWave Epic IRE Assessment** is a structured, healthcare-specific evaluation designed to answer that question with clarity and evidence.

CloudWave assesses an organization's ability to recover Epic using an **Isolated Recovery Environment (IRE)** pattern, aligned with Epic guidance and emerging regulatory direction. The engagement focuses on cyber recovery readiness, not infrastructure theory or generic disaster recovery assumptions.

Through deep discovery, dependency mapping, and facilitated criticality analysis, CloudWave identifies what is required to restore Epic safely within the first 72 hours of a cyber incident, what gaps exist today, and what must change to make recovery executable.

The assessment delivers a **board-ready**, technically defensible roadmap that prioritizes actions, clarifies clinical, operational, security, and executive decision ownership during Epic cyber recovery—reducing ambiguity when time-critical decisions must be made under attack conditions.

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 **gocloudwave.com**

CloudWave

ASSESSMENT OBJECTIVES

The Epic IRE Assessment is designed to:

- Confirm Epic recoverability in a cyber event, not only in traditional DR scenarios.
- Define the **minimum viable Epic footprint** required to support safe patient care during disruption.
- Identify dependencies that determine recovery success or failure, including identity, network, storage, interfaces, and third-party systems.
- Evaluate readiness against key HIPAA Security Rule NPRM expectations, including:
  - 72-hour restoration procedures
  - Documented criticality analysis
  - Backup recency and integrity
  - Ongoing testing and evidence requirements
- Deliver a prioritized roadmap with clear next steps and decision points.

KEY OUTCOMES

Organizations completing the CloudWave Epic IRE Assessment gain:

- **Clear visibility into cyber recovery risk**, specific to Epic, not generic infrastructure.
- **Reduced recovery uncertainty** through documented dependencies and restoration sequencing.
- **Executive-level confidence** via a defensible recovery strategy aligned to Epic guidance.
- **Improved audit and regulatory readiness** through mapped evidence and documented procedures.
- **Operational clarity** on what must be restored in the first 72 hours versus what can wait.
- **Actionable next steps**, prioritized by clinical impact and recovery feasibility.

WHAT CLOUDWAVE DELIVERS

CloudWave provides a complete assessment package in editable formats, including:

- **Executive Readout (10–15 slides):** Current state, top risks, IRE options, recommended path, and decisions required.
- **Epic IRE Assessment Report (Detailed):** Environment overview, dependency map, gap analysis, and prioritized recommendations.
- **IRE Target-State Blueprint (Assessment-Level):** Reference architectures, isolation concepts, activation model, and operating approach.
- **HIPAA Readiness Mapping Appendix:** Alignment of current state and recommendations to proposed 72-hour recovery and criticality expectations.
- **Testing and Runbook Outline:** Practical testing strategy, evidence checklist, and activation flow.

These deliverables are designed for use by IT leadership, security teams, clinical operations, and executive stakeholders.

CloudWave provides a complete assessment package in editable formats. These deliverables are designed for use by IT leadership, security teams, clinical operations, and executive stakeholders.

100 Crowley Drive, Marlborough, MA 01752 877-991-1991 **gocloudwave.com**

CloudWave

SERVICE HIGHLIGHTS

- Structured Epic and infrastructure discovery
- Cyber-focused recovery analysis, not traditional DR assumptions
- Criticality workshop and minimum viable Epic definition
- Dependency mapping across identity, network, storage, and interfaces
- IRE isolation and activation strategy options
- Practical testing and evidence guidance
- Board- and audit-ready documentation
- Healthcare-aligned security and privacy handling

WHY CLOUDWAVE

CloudWave brings deep, hands-on ownership of healthcare infrastructure and Epic environments. This assessment is delivered by practitioners who support EHR platforms daily and understand how recovery decisions directly impacts patient safety, access to care, clinician productivity and revenue continuity.

The CloudWave Epic IRE Assessment is not a compliance checkbox or generic architecture exercise. It is a practical, healthcare-specific engagement designed to produce clarity, confidence, and executable outcomes for organizations preparing for modern cyber threats to support patient safety during a cyber disruption.

LEARN MORE AT gocloudwave.com | 877-991-1991

About CloudWave

CloudWave is a full-service cybersecurity and cloud services provider exclusively for healthcare. Protecting over 300 hospitals and health systems, CloudWave delivers end-to-end solutions combining secure hosting, IT operations, and 24/7 threat detection. Services include managed security, risk and compliance, disaster recovery, and cloud optimization—all with a healthcare-first approach. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Center, CloudWave provides healthcare organizations with a cyber-ready foundation for safe, uninterrupted patient care.