STRATEGIC BENCHMARK REPORT | OCTOBER 16, 2026

2026 Healthcare IT Resilience Benchmark

Practices, Evidence and Priorities for High-Availability Health Systems

A strategic framework to assess critical workflows, demonstrate safe recovery, and prioritize resilience investment.

The executive test

Can critical care continue during disruption? Can essential services recover within approved tolerances? What evidence demonstrates both?

For U.S. health system CIOs, CTOs, CMIOs, COOs, security leaders, clinical operations teams, and governing boards.

BENCHMARK BASIS

Compare critical services against recommended practices, locally approved objectives, and their own demonstrated performance over time. An evidence-informed CapMinds assessment framework, not a national hospital ranking or certification.

Research cut-off: October 16, 2026.

01 / EXECUTIVE ASSESSMENT

Make care continuity the investment test

Infrastructure can be available while medication orders, diagnostic images, or critical results remain inaccessible. Leadership needs evidence that the complete clinical workflow operates correctly and can recover safely when one of its dependencies fails.

Three priorities for leaders

Approve service-specific disruption and data-loss tolerances. Test clinical continuity alongside technical restoration. Direct funding to demonstrated gaps with the greatest clinical consequence and shared exposure.

Current guidance reinforces operational readiness

Joint Commission's voluntary Cyber Resilience Readiness (CRR) program addresses clinical continuity during extended technology outages. Its current components include self-assessment, expert review, advisory services, and certification managed by Joint Commission. Self-assessment completion does not confer certification.

Dependency failures extend beyond the hospital

AHA's March 2024 Change Healthcare survey of approximately 1,000 responding hospitals found 94% reported financial impacts and 74% reported direct patient-care impacts. These historical respondent findings demonstrate supplier exposure; they are not 2026 national prevalence estimates.

Published findings and proposed benchmarks serve different roles

NIST, HHS, SAFER, ASPR TRACIE, and HSCC inform the practices in this report. Its measures, maturity rubric, prioritization rules, and worked example are CapMinds proposals for local use. The public Censinet 2026 study summary identifies 54 organizations but does not establish national availability or recovery-time percentiles.

How to use this report

Select critical workflows, approve objectives with clinical owners, collect evidence, and run controlled exercises. Use the scorecard to identify gaps; use the decision framework to assign actions and funding. Compare repeat results only when scope and measurement rules remain consistent.

Scope: EHR and integrations, identity, infrastructure, suppliers, facilities and enabling technology, clinical downtime, and recovery reconciliation. No original hospital survey or comparative claim about top-performing systems is made.

02 / BENCHMARK METHOD

Define what is being compared

This is a practice-based and objective-based benchmark.

It compares an organization's capability with published recommendations, approved service tolerances, and its prior test results. It does not assign a national percentile.

Step	Required decision and evidence
1. Bound the service	Name the clinical workflow, sites, operating hours, demand assumptions, upstream and downstream systems, and accountable clinical owner.
2. Set objectives	Use a business impact analysis to approve maximum tolerable disruption, recovery time objective (RTO), recovery point objective (RPO), and minimum service during downtime.
3. Define the test	Specify scenario, representative load, participants, safety controls, start/stop conditions, clocks, acceptance checks, and evidence capture.
4. Assess outcomes	Compare observations with the preapproved criteria. Record pass, fail, or unverified for each capability. Assess maturity separately.
5. Act and repeat	Assign an owner, deadline, interim control, and acceptance authority for each material gap. Retest after remediation or relevant change.

Evaluate eight domains

Clinical criticality; infrastructure and access; backup and restoration; security containment; integration integrity; clinical continuity; supplier and regional coordination; governance and improvement. Record site-specific exceptions rather than averaging them away.

Distinguish three outcomes

Pass: observed evidence meets the stated criteria.
Fail: evidence shows a criterion was missed.
Unverified: evidence is absent, stale after a relevant change, or does not cover the scenario. A documented plan alone cannot establish a passing operational outcome.

Source foundation: NIST SP 800-34 Rev. 1 provides guidance on business impact and contingency planning. The proposed assessment method extends that foundation to healthcare workflows; the eight domains and outcome labels are not an official NIST scoring system.

03 / PRACTICE COMPARISON

Translate resilience into observable practice

These contrasts describe stronger assurance, not measured differences between ranked hospitals. Assess the operating evidence behind each claim.

Dimension	Limited assurance	Stronger assurance
Clinical priorities	Important applications are listed.	Workflow tolerances and minimum service levels are approved; dependencies and sites are identified.
Architecture	Duplicate components exist.	Scenario tests demonstrate alternate capacity, access, and independence from the failed dependency.
Recovery	Backup jobs complete.	Restore evidence establishes usable data, acceptable recovery time, security checks, and service-owner approval.
Integration	Endpoints respond.	Orders and results complete correctly; queue age, failures, duplication, and reconciliation are evaluated.
Clinical continuity	Downtime procedures exist.	Staff demonstrate patient identification, substitute workflows, handoffs, communication, and escalation.
Supplier continuity	An SLA is signed.	Vendor-loss exercises verify alternatives, contacts, access, responsibility boundaries, and recovery evidence.
Governance	Risks appear on a register.	Leaders approve actions, funding, deadlines, and residual-risk ownership; follow-up verifies the result.

What the sources contribute

SAFER System Management addresses integrated testing, interface monitoring, and change safety. HHS cybersecurity goals provide voluntary control priorities. HSCC's OCCI checklist supports enterprise operational coordination. These practices should be translated into local acceptance tests, not used as a substitute for them.

Investment question

Which failure will this investment address, which critical workflows benefit, and what test will demonstrate that the exposure has reduced?

04 / TECHNICAL RESILIENCE

Test failures across the dependency chain

Inventory applications, data, identity, networks, interfaces, facilities, and suppliers. High availability, disaster recovery, and cyber recovery need distinct scenario tests: surviving a component fault does not establish recovery from corruption or compromise.

Scenario	Required exercise evidence
Identity or access loss	Approved alternate access is usable by authorized staff; privileges and audit records are checked.
Compute, database or site loss	Alternate capacity works under the stated load; data consistency, application access, and return-to-primary procedures are verified.
Interface interruption	Queued transactions are accounted for. Restart and replay controls prevent unexplained loss, duplication, or misassociation.
Ransomware or corruption	Restoration assets are checked for compromise and integrity; recovery occurs in an approved environment before reconnection.
OT or enabling-system loss	Facilities and safety owners verify minimum operation, vendor access dependencies, safe isolation, and reconnection conditions.
Critical supplier loss	Operational teams activate approved alternatives; constraints, escalation contacts, and restoration ownership are demonstrated.

Test separation and safe isolation

CISA's July 28, 2026 CI Fortify bulletin emphasizes mapping connections, separation points, and tested graduated isolation plans. Apply these principles with clinical and facilities owners. Test effects on remote support, identity, communications, and dependent services before authorizing isolation in live operations.

Treat OT guidance according to its scope

NSA's October 8, 2026 release concerns zero trust for OT, primarily in national-security and defense environments, with broader applicability for IT and OT leaders. Evaluate relevance to hospital enabling systems; it is not a healthcare-specific compliance mandate.

NIST SP 800-61 Rev. 3 supports verification of recovery assets and restored services. Proposed controls such as shared-credential checks and clinical reconnection gates require architecture-specific design and safe change approval.

05 / CLINICAL CONTINUITY

Make the substitute workflow usable

Approve the minimum sustainable service

Clinical leaders define what continues, what changes, and what pauses during a particular failure. Include patient identification, medication administration, diagnostics, transfers, staffing, and time-sensitive follow-up. State the capacity and staffing assumptions behind the plan.

Observe staff executing the plan

ASPR TRACIE's Hospital Downtime Preparedness Checklist covers departmental planning and resources. Use a controlled exercise to verify access to forms, approved offline information, supplies, contacts, and equipment instructions. Include a shift handoff and an urgent result.

Keep communication available

SAFER Contingency Planning recommends downtime communications independent of EHR infrastructure. Prove the actual alternative works during the chosen identity, network, or site failure. Confirm who declares downtime and how frontline teams receive status updates.

Prepare for prolonged interruption

AHA's September 30, 2026 resilience commentary recommends preparedness for safe care for 30 days or longer without connected technology. Use this as a stress scenario for staffing, supply, access, and service modification; it is not an acceptable outage allowance or a recovery deadline.

Coordinate beyond the affected organization

HSCC's OCCI checklist supports extended enterprise outage response. A JAMA Network Open study published in 2023 found increased ED demand and other disruptions at two neighboring hospitals during a 2021 ransomware event. Plan regional communications and patient transfer decisions; that study does not establish a universal effect size.

Use CRR resources appropriately

Joint Commission's voluntary CRR program provides a relevant clinical continuity assessment resource. This report does not reproduce its standards, determine eligibility, or award certification. Use official program materials for those purposes.

Exercise safety: agree test boundaries, supervision, stop conditions, and clinical escalation in advance. Simulated workflows and representative test records should be used where possible.

06 / PERFORMANCE SCORECARD

Pair each measure with a passing criterion

The criteria below are proposed templates. Approve numeric limits locally before testing. Report results by service, site, scenario, and measurement window; preserve failed and timed-out attempts in the denominator.

Measure	Evidence and definition	Acceptance rule
Workflow success	Correct eligible completions / all eligible attempts; verify identity, content, destination, and latency.	Meets approved success target; any safety-critical error fails the applicable safety gate.
Response time	95th-percentile completion time; separately count failures and timeouts.	Within the approved latency limit under the specified load.
Service recovery	Time from agreed disruption start to validated clinical availability. Retain milestone timestamps.	Within service RTO using matching clock boundaries.
Data recovery	Latest consistent recovered data point; quantify the loss interval and missing transactions.	Within RPO; safety-critical records reconciled or covered by approved controls.
Restore coverage	Services with current passing restore evidence / all in-scope critical services.	Meets approved coverage target; identify every uncovered service.
Continuity activation	Elapsed time to usable substitute workflow; observe staffing and minimum capacity.	Activation limit and minimum service level both met.
Isolation readiness	Observed operation after specified connections are removed, with safety approval.	Essential service and reconnection criteria met.
Backlog and actions	Open reconciliation items and corrective findings by risk, owner, age, and due date.	No overdue critical items; remaining exceptions explicitly controlled and assigned.

Do not combine unlike tests into one enterprise percentage. Specify exclusions and any maintenance windows. Record the evidence date, system version, load, and exceptions.

Availability is one measure

For a 365-day, 24/7 period, 99.9% corresponds to 8h 45m 36s unavailable time; 99.99% to 52m 33.6s; 99.999% to 5m 15.36s. These are calculations, not healthcare standards. Evaluate functional degradation and partial failures separately.

07 / RECOVERY ACCEPTANCE

Record three distinct recovery milestones

NISTSP800-61 Rev.3 calls for recovery integrity checks, service restoration validation, and confirmation of normal operation. Translate these into explicit technical and clinical acceptance gates.

Milestone	Required acceptance evidence	Accountable approval
Technical restoration	Required infrastructure and application components operate; security and data-integrity checks meet the approved recovery plan.	Technical recovery lead, with security approval where compromise is involved.
Validated clinical availability	Authorized users complete specified end-to-end workflows correctly at acceptable performance; critical interfaces and patient associations are verified.	Clinical service owner with application and integration leads.
Operational reconciliation	Downtime records, orders, results, identifiers, messages, and billing items are reconciled; outstanding exceptions have safe controls and owners.	Clinical operations and relevant departmental owners.

Use compatible clocks

Define the disruption start consistently. If local RTO measures technical restoration, report that comparison separately from time to validated clinical availability. Set an explicit clinical availability objective. Maximum tolerable downtime constrains disruption to the business or clinical process; it is not identical to a system RTO.

Reconcile before closing the incident

Keep the technical recovery time, clinical availability time, and reconciliation completion time visible. The incident may remain open after services return. Do not describe backlog closure as part of a met RTO unless that objective explicitly includes it.

Data protection needs its own evidence

RPO concerns the recoverable data point and loss tolerance. A recent backup timestamp alone does not prove consistency or usable clinical records. Validate the recovery point, measure missing transactions, and account for documentation created during downtime.

Source foundation: NIST SP 800-34 Rev. 1 for RTO/RPO and business impact planning; NIST SP 800-61 Rev. 3 for recovery validation. Milestone names and approval roles above are proposed local governance conventions.

08 / WORKED ASSESSMENT

Example: urgent laboratory result delivery

Hypothetical exercise only. All targets, timings, counts, and maturity judgments on this page are illustrative. They are not observed hospital results, clinical turnaround standards, or national benchmarks.

Scope: one hospital, EHR-to-LIS orders and result return through an integration engine. A simulated engine failure interrupts electronic delivery. Laboratory processing continues; the exercise tests ordering, result routing, escalation, and reconciliation.

Preapproved local objective	Observed exercise result	Assessment
Activate approved downtime workflow within 10 minutes.	Usable at 7 minutes; staff demonstrate patient identification and result read-back.	Pass
Restore validated electronic workflow within 60 minutes of disruption.	Technical restoration at 42 minutes; validated clinical availability at 75 minutes.	Fail: service RTO missed by 15 minutes.
Recover consistent engine data with no more than 15 minutes of data loss.	Queue records account for all persisted messages; no loss observed in the tested scope.	Pass for tested scope; not proof of all-scenario recovery.
All 120 test transactions correctly associated and routed; no safety-critical errors.	Initial validation: 118 pass; 2 duplicate results. Replay corrected and all 120 revalidated by minute 75.	Initial fail; retest pass. Preserve the original failure.
Reconcile all 24 downtime records within 180 minutes.	All 24 matched and closed by minute 150.	Pass; separate from service recovery.

Decision and ownership

Integration owner corrects replay handling and adds duplicate-detection validation. Application owner and clinical lead establish a timed end-to-end acceptance checklist. Clinical owner retains the approved downtime workflow. Retest both fault scenarios under representative load before closing the findings.

Maturity interpretation: continuity may reach Level 3 for the exercised scenario. Integration integrity remains Level 2 pending a full repeat scenario after the replay fix; the targeted transaction retest alone is insufficient. A passing retest does not erase a missed recovery objective or justify an enterprise-wide maturity claim.

09 / MATURITY AND GOVERNANCE

Assess demonstrated capability by domain

Assign maturity to each service and scenario using the highest level fully supported by evidence. Report the domain profile alongside pass/fail/unverified outcomes. These proposed levels are not a validated national scoring instrument.

Level	Minimum evidence
0 Unestablished	No approved approach. Record missing evidence as unverified; do not infer a proven operational failure.
1 Defined	Named owner, documented method, and approved service objectives.
2 Implemented	Resources and controls are deployed; roles are understood. Demonstration is absent or does not yet meet criteria.
3 Demonstrated	A relevant test or incident meets preapproved acceptance criteria; evidence and exceptions are retained.
4 Sustained	Repeated evidence under relevant change; corrective actions closed; recurring performance reviewed by accountable leaders.

Make evidence traceable

Retain service/sites; scenario; dependency and version scope; evidence date; approved objective; observed result; outcome; maturity; clinical and business consequence; owner; interim control; due date; and approval authority.

Escalate critical exceptions

Escalate absent tolerances, unproven restores, unsafe substitute workflows, safety-critical data errors, and missing acceptance owners. Avoid averaging these away. A strong aggregate score cannot compensate for a critical workflow that fails its safety gate.

Keep risk acceptance within authority

Clinical, security, and executive owners should document residual exposure and interim safeguards where continued operation is permissible. Risk acceptance does not waive legal obligations or authorize unsafe care. Compliance and clinical safety teams must determine applicable constraints.

Separate compliance from readiness

As reviewed October 16, 2026, HHS continues to describe the Security Rule update as an NPRM and states that the current rule remains in effect during rulemaking. Maintain a change register for official final rules, effective dates, applicability, and accountable action owners.

10 / INVESTMENT AND ACTION PLAN

Fund the gaps with the greatest consequence

Prioritize by clinical consequence and time sensitivity, shared dependency exposure, and demonstrated failure. Then compare remediation effort, delivery constraints, and residual risk. Avoid invented financial precision or a weighted score that conceals an urgent safety issue.

Priority	Decision rule	Evidence for funding
Immediate	Safety-critical failure or uncontrolled disruption to time-sensitive care.	Clinical impact, interim safeguards, decision authority, and a timed remediation/retest plan.
Next	Shared dependency can disable several critical workflows; recovery is unverified or misses tolerance.	Affected service map, common failure path, options, and acceptance test.
Planned	Capability works, but repeatability, observability, capacity, or support needs improvement.	Trend evidence, remaining risk, cost/effort range, and measurable improvement objective.

Period	Deliverable	Accountable leads
Days 1-30	Select workflows; approve tolerances and minimum service; map OT and supplier dependencies; baseline outcomes and maturity.	CIO, CMIO, COO; service owners approve scope.
Days 31-60	Exercise restore, continuity, isolation, and supplier loss in controlled scope; record three recovery milestones and reconcile records.	IT operations, security, integration, facilities, and clinical operations.
Days 61-90	Remediate and retest urgent gaps; approve residual-risk decisions; fund the next tranche and establish review cadence.	Executive sponsor and service owners; board oversight as appropriate.

Present an investment decision, not a technology wish list

For each proposal, show affected services, observed gap, clinical and financial exposure, options, estimated cost range with assumptions, delivery owner, acceptance test, and consequence of deferral. Compare options that address the same risk.

Start with one workflow: complete its evidence record and run the first controlled exercise. Expand after the method produces decisions that clinical, technical, and operational owners can defend. The 90-day sequence is a proposed program plan, not a completion guarantee.

11 / REFERENCES

Source register and research notes

Official and primary evidence underpinning the report. Links are clickable. Current status sources checked October 16, 2026; historical studies retain their original dates.

HealthIT.gov. 2025 SAFER Guide: Contingency Planning. 2025 edition; PDF internally dated August 2024. Open source **HealthIT.gov.** 2025 SAFER Guide: System Management. 2025 edition. Open source

NIST. SP 800-160 Vol. 2 Rev. 1: Developing Cyber-Resilient Systems. 2021. Open source

HHS. Healthcare and Public Health Cybersecurity Performance Goals. Voluntary guidance. Open source

American Hospital Association. Making Headway Toward Cyber Resilience. September 30, 2026. Open source **American Hospital Association.** Change Healthcare impact survey. March 15, 2024; approximately 1,000 responding hospitals. Open source

Censinet. 2026 Healthcare Cybersecurity & AI Benchmarking Study: public executive-summary landing page; 54 organizations. Full study methodology was not independently assessed. Open source

NIST. SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. 2010. Open source

Health Sector Coordinating Council. Operational Continuity - Cyber Incident (OCCI). April 2022. Open source

NIST. SP 800-61 Rev. 3: Incident Response Recommendations. April 2025; recovery guidance RC.RP-03 through RC.RP-06. Open source

HHS ASPR TRACIE. Hospital Downtime Preparedness Checklist. Departmental continuity planning resource. Open source

Dameff et al., JAMA Network Open. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. May 8, 2023. DOI: 10.1001/jamanetworkopen.2023.12270. Open source

Joint Commission. Cyber Resilience Readiness program. Current voluntary program components and certification distinctions. Open source

NSA. Zero Trust Guidance for Protecting Operational Technology Systems. October 8, 2026; primarily national-security and defense guidance. Open source

CISA. Joint guidance on isolating vital OT and enabling systems during crisis. Official bulletin, July 28, 2026. Open source **HHS OCR.** HIPAA Security Rule NPRM. Current rule remains in effect during rulemaking; status checked October 16, 2026. Open source

Interpretation limits: guidance describes recommended practices; it does not establish causal performance differences among health systems. Historical incident findings are dated explicitly. Proposed assessment metrics and levels require local validation. This report does not provide a compliance determination.