ECRI | The Most Trusted Voice in Healthcare

Digital Darkness
Preparing for the Inevitable

Proactive strategies for HTM professionals to maintain operational resilience when technology access fails

MDEXPO

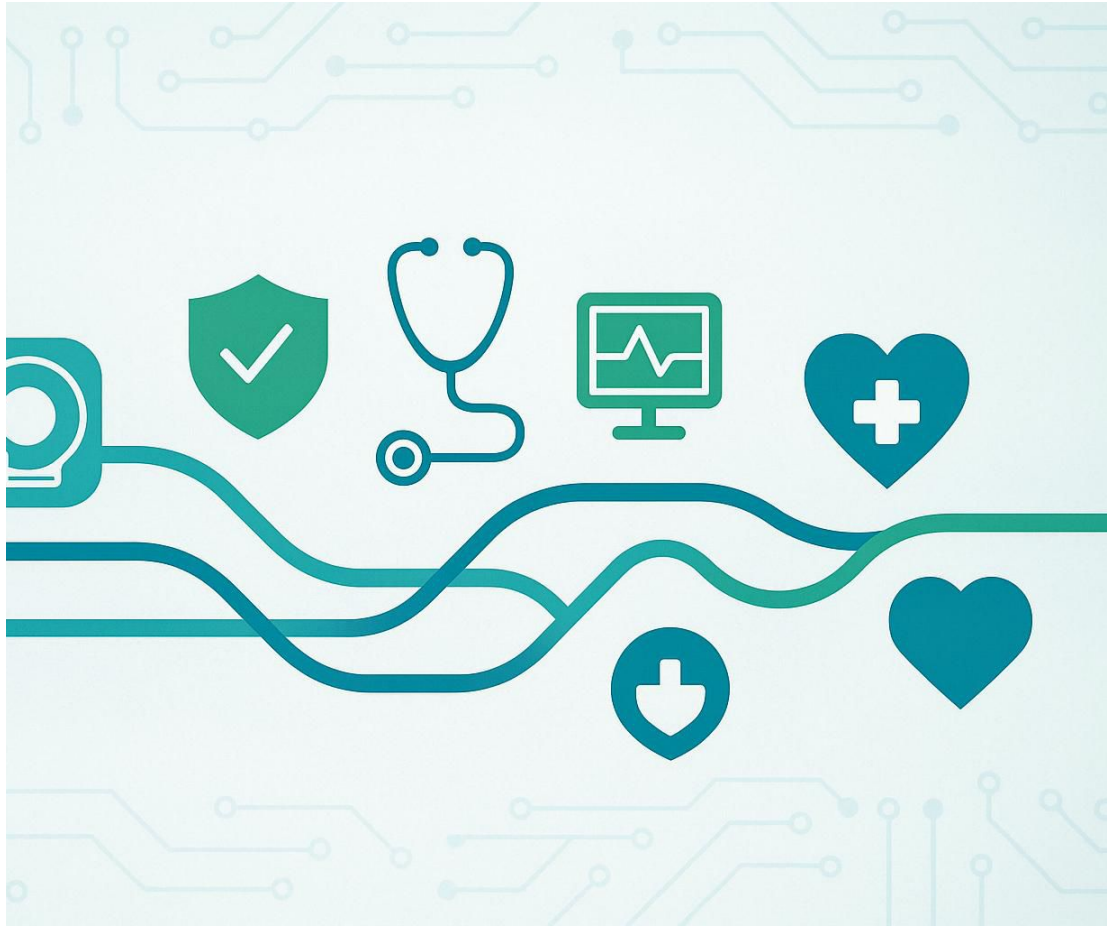


©2026 ECRI | MD Expo Baltimore

About ECRI

ECRI: Your Trusted Healthcare Technology Partner

- Independent, nonprofit organization
- 50+ years improving patient care safety
- Evidence-based guidance for healthcare technology
- Cybersecurity expertise in medical device management



©2026 ECRI | MD Expo Baltimore

THE JOURNEY AHEAD



Objective: Equip HTM professionals with proactive strategies to maintain organizational resilience during large-scale technology outages.

- **01 — THE WHY:** Define Digital Darkness — what it is, what it looks like in a hospital, and why it matters to every HTM professional
- **02 — THE WHAT:** Six categories of events that cause Digital Darkness — and how they combine into cascading, multi-vector incidents
- **03 — THE HOW:** The proactive approach — building your preparation playbook, documentation package, and DR/BC framework before you need it
- **04 — THE RESULT:** Full recovery — how to turn the lights back on without creating new problems, organized by event type

Key principle: Everything in this session should integrate into your organization's existing disaster preparedness plan — or become the catalyst for creating one if it does not exist.

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

01
The Why: Digital Darkness

What happens when every screen goes black?

© 2026 ECRI | MD Expo Baltimore

WHAT IS DIGITAL DARKNESS?

The sudden, complete loss of electronic communication, internet connectivity, and digital infrastructure — creating a technology blackout across your facility.

| EHR crashes mid-chart | Monitors go dark | Badge readers freeze | Pumps lose network sync |

Are you prepared for what comes next?



MDEXPO

ECRI ©2026 ECRI | MD Expo Baltimore

02
The What: Events That Cause It

Six threat categories — and they don't come alone.

© 2026 ECRI | MD Expo Baltimore

THREAT LANDSCAPE

What events could plunge your organization into Digital Darkness?

Cyberattacks Ransomware, social engineering, phishing, unauthorized access through compromised systems	**Vendor Outages** EMR/EHR cloud hosting outages, third-party service failures due to any of these circumstances
Natural Disasters Hurricanes, earthquakes, tornadoes, wildfires, snowstorms — causing physical and infrastructure damage	**Internal System Failures** Network equipment failures, phone/communication system failures, power failures with lack of redundancy or failed generators
Terrorism Attacks on infrastructure, power grids, bridges, hospitals, and populated areas that disrupt healthcare operations	**Insider Threats** The potential for an insider to use their authorized access or understanding of an organization to harm that organization

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

THREAT LANDSCAPE

What events could plunge your organization into Digital Darkness?

⚠ **Combination events:** These threats rarely happen in isolation. A natural disaster can simultaneously trigger internal system failures, vendor outages, AND communication breakdowns. Your preparedness plans must account for cascading, multi-vector events.

Integration point: Digital darkness preparedness should be integrated into your organization's general disaster preparedness plan. If that plan does not exist, this is your catalyst to create one.



MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

QUICK POLL — Where Does Your Organization Stand?

Raise your hand if...

1. **Your organization has a documented downtime plan for HTM** — Written procedures that your team can execute when digital systems fail
2. **You've actually tested that plan in the last 12 months** — A tabletop exercise, simulation, or drill — not just a read-through
3. **You know which devices in your facility are on generator-backed circuits** — You can identify right now which critical equipment stays powered during an outage

The gap between these answers is exactly what the rest of this session is designed to close.

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

03 — THE HOW

Proactive Preparation

Build the playbook before you need it.

© 2026 ECRI | MD Expo Baltimore

THE MINIMUM VIABLE HOSPITAL

When systems go down, what MUST keep running to keep patients safe?

Think of this as supporting the "minimum viable hospital" protocol — the life-safety and clinical operations that must be restored first to ensure patient safety.

RESTORE FIRST (Priority Systems):

- Ventilators and life support systems
- Patient monitoring systems (bedside monitors, telemetry, central stations)
- Infusion pumps (IV, syringe, PCA, enteral feeding)
- Lab analyzers and lab automation systems
- EMR/EHR access (clinical documentation,

KEY QUESTIONS TO ANSWER BEFORE AN EVENT:

- How is each critical system powered — UPS battery backup, generator, or standard outlet?
- Which devices are on emergency generator-backed circuits (red outlets)?
- What is the manual fallback if the device fails entirely — and where is that documented?
- Where are the paper-based downtime procedures stored — and are they current?
- Who owns each system's recovery — HTM, IT, facilities, or a vendor?

Critical action: If monitors or networked devices fail, staff must initiate manual monitoring or transition to battery-backup devices immediately. This transition must be practiced before an event — not during one.

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

HTM PREPARATION CHECKLIST

Disaster Recovery and Continuity Planning: Preparation and Prevention for HTM



Asset Inventory and Prioritization: Maintain a complete list of all medical equipment including device location, network dependencies, and power source. Flag critical and high-risk items for priority recovery. This inventory becomes your triage list during an event.

Power Supply Audit: Review all essential equipment and confirm it is connected to emergency, generator-backed circuits — sometimes identified by a red power outlet. Priority systems to verify: ventilators, infusion pumps, patient monitors, lab analyzers, and any networked clinical system.

Battery Maintenance and Audit: Test and replace batteries on a regular cadence — recommended 6-month cycle — for portable devices, monitors, and emergency kits. Document how long each device battery lasts under load. Battery runtime determines your response timeline and dictates how quickly manual alternatives must be deployed.

Emergency Monitoring Kits: Designate and pre-stage emergency monitoring kits for critical areas including OR, ICU, and surgery suites. Kits should include backup flashlights, manual blood pressure cuffs, battery-operated pulse oximeters, and manual or battery-operated medical devices. Kits should be checked quarterly and restocked immediately after use.

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

DOCUMENTATION THAT SURVIVES THE OUTAGE

If it is only digital, it does not exist during Digital Darkness.

Manual Override Procedures: Document manual overrides for equipment like ICU beds, patient lifts, and motorized equipment. Include step-by-step instructions that staff can follow without electronic access. These procedures should be tested during drills.
Cold Storage and Laboratory Contingency: Document and prepare plans for the loss of laboratory cold storage. Prepare dry ice coolers or backup power connections for critical laboratory refrigeration systems. Include temperature monitoring protocols and maximum allowable outage durations for each storage type.
Laminated Downtime Procedures: Create clear, per-device downtime procedures and store them in a known, accessible location on each unit. Laminating protects the content from damage. Include power source identification, manual intervention instructions, and a contact list for each device's vendor or responsible team.
Communication Plan: Coordinate with facility management to ensure generators are not pushed beyond their rated capacity, networks are assessed for availability, and alternate communication systems — radios, runners, overhead PA — are available for staff when digital communication fails.
Safety Checks for Hazardous Materials: Incorporate safety checks to safely secure and store chemical, hazardous materials, or sensitive equipment if HVAC or fume hoods fail during an outage. Include evacuation triggers for areas that become unsafe.



MDEXPO
ECRI
©2026 ECRI | MD Expo Baltimore

DISASTER RECOVERY & BUSINESS CONTINUITY



The organizational framework that wraps around your HTM-specific preparations:

- **Communication Plan:** Documented procedures that notify employees, patients, media — and in some circumstances, law enforcement. Must include a chain of command, escalation paths, and designated spokespersons. Determine in advance who communicates what, to whom, and through which channels.
- **Roles and Responsibilities:** Clearly defined, documented roles and tasks for all team members during an incident. Build a RACI matrix — Responsible, Accountable, Consulted, Informed — for each critical system and each scenario type. If people do not know their role before the event, they will not find it during the event.
- **Incident Response and Recovery Procedures:** Detailed step-by-step procedures for detecting, containing, and eliminating threats, and restoring data and systems. These are your operational playbooks — specific to each event type, regularly reviewed, and accessible in both digital and physical formats.
- **Testing and Updates:** Simulate tests — tabletop exercises, functional drills — to validate plan effectiveness. If gaps or failures are identified, update immediately. Plans must be reviewed and updated at minimum annually to remain effective against emerging threats. An untested plan is a hope, not a plan.

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

THE HARD TRUTH ABOUT PREPARATION

Most digital darkness events arrive without warning.

When it comes to Digital Darkness, it is very unlikely you will know an incident is coming. Some natural disasters offer advance warning — hurricanes, winter storms — but cyberattacks, internal failures, vendor outages, and insider threats arrive without notice. Since the likelihood of advanced warning is low, we must equip ourselves with proactive plans, procedures, and backup systems.

Your team's readiness is determined by what you have built before the event — not during it.



MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

THE HARD TRUTH ABOUT PREPARATION



Plans are your map	Practice is your muscle memory	Updates keep you current
Written procedures guide your team through chaos when clear thinking is hardest	Tabletop exercises and drills build the reflexes your team needs under pressure	Annual reviews ensure your plans cover new technology, new threats, and organizational changes

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

04 — THE RESULT
Full Recovery

Turning the lights back on — without making it worse.

© 2026 ECRI | MD Expo Baltimore

COMMON RECOVERY PITFALLS

What are some common pitfalls to avoid before you restore?

- ✕ **Assuming data backups are clean and uncompromised** While offline and offsite backups are generally protected from ransomware, backups stored in a network-reachable location fall within the risk scope of cyberattacks. Any backup that was accessible from the compromised network must be validated before restoring. Restoring from an infected backup reinfects your systems.
- ✕ **Failure to update disaster and continuity plans as infrastructure evolves** Recovery plans need to be reviewed and updated on a schedule — at least annually. A recovery plan written for your 2022 infrastructure does not protect your 2026 reality — new cloud services, new devices, new network architecture all create gaps.
- ✕ **Lack of training for employees on disaster procedures** Untrained staff will struggle to be effective in an emergency scenario. If people have not practiced the procedures in a tabletop exercise or functional drill, they will not execute them effectively under the stress and time pressure of a real event. Training must be recurring, not one-time.



MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

RECOVERY PLAYBOOK BY EVENT TYPE: RANSOMWARE



How you recover depends on the type of event. Here are the key steps for each:

RANSOMWARE:

- IT and cybersecurity teams lead recovery; HTM team is assigned specific restoration tasks
- **Validate backups:** Restore systems from known good, secure backups — confirm they are ransomware-free before any restoration begins
- **Phased system restoration:** Prioritize critical systems first — patient monitors, infusion pumps, lab systems, EMR/EHR
- **Data integrity check:** Migrate data generated during downtime (paper records, manual logs) into digital systems to ensure continuity of the patient record
- **Credential reset:** Force password resets for affected users and identify where multi-factor authentication can be enabled if not already in place

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

RECOVERY PLAYBOOK BY EVENT TYPE: NATURAL DISASTER



NATURAL DISASTER:

- Entire organization assists with post-event recovery; depending on severity, this could be an extended, multi-day or multi-week exercise
- **Damage assessment and isolation:** Evaluate physical infrastructure, systems, and network connectivity before powering anything back on; isolate damaged or compromised systems to prevent further data loss
- **Device safety verification:** Inspect medical equipment for physical damage, water intrusion, or environmental exposure before returning to clinical use
- **Transition from downtime procedures:** Carefully transition from manual procedures back to digital operations ensuring no patient data is lost during the switch

MDEXPO

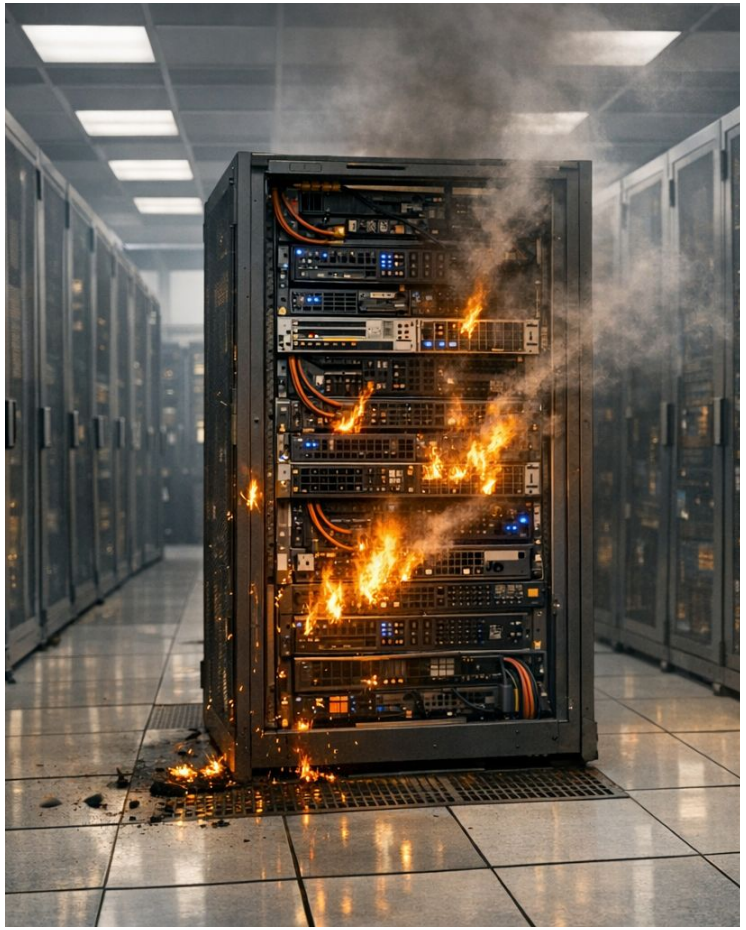
ECRI

©2026 ECRI | MD Expo Baltimore

RECOVERY PLAYBOOK BY EVENT TYPE: INTERNAL FAILURE

INTERNAL FAILURE:

- IT and infrastructure teams restore failed equipment or activate redundant systems; turnaround may be quick or lengthy depending on the failure scope
- **Phased reconnection:** Prioritize critical clinical systems for patient safety before administrative systems
- **Data migration and validation:** Transition manual and paper-based data generated during downtime back into digital systems with verification
- **Root cause analysis:** Determine what failed, why it failed, and what changes prevent recurrence



MDEXPO

ECRI ©2026 ECRI | MD Expo Baltimore

UNIVERSAL RECOVERY PRINCIPLES

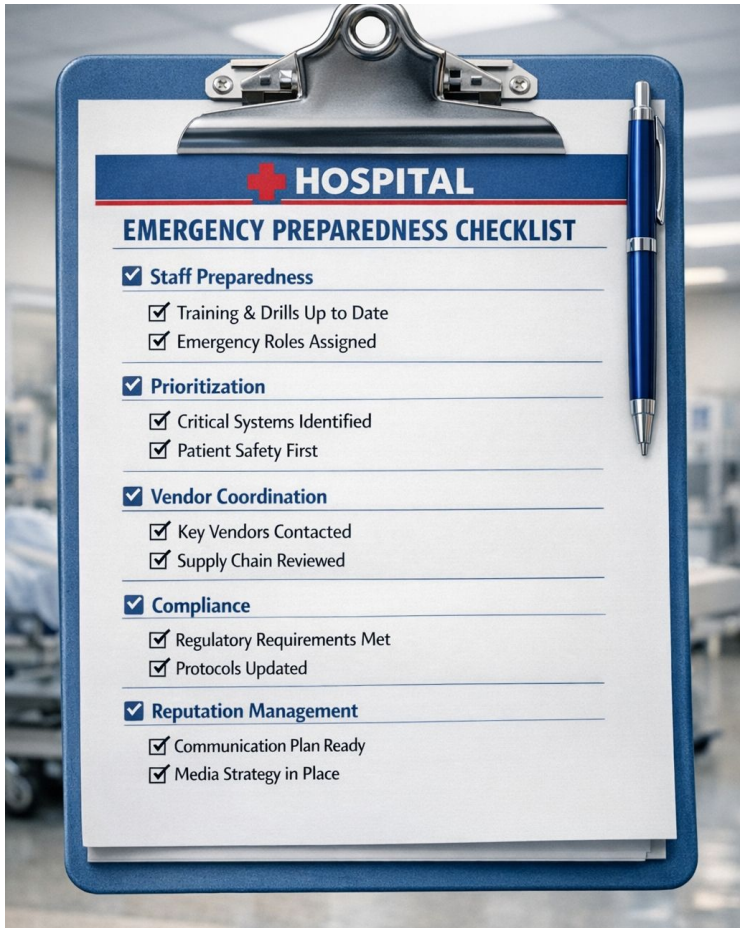
Staff Preparedness: Ensure staff are properly trained in both downtime procedures AND the rollback to digital operations after the incident. Training must cover both directions — going offline and coming back online — because the risks are different in each direction.

Prioritization: Always focus on restoring critical and essential clinical systems first — monitors, ventilators, infusion pumps, lab systems — before administrative systems are restored. Patient safety drives the restoration sequence.

Vendor Coordination: Work closely with third-party vendors and IT staff to restore cloud services once networks are back online. Have vendor contact information, escalation paths, and service level agreements documented and accessible in physical format before an event occurs.

Compliance: Work with legal and compliance staff to maintain HIPAA and other regulatory requirements during the recovery process. Recovery chaos creates temptation to cut corners on patient data handling — do not. Document compliance steps throughout.

Reputation Management: Communicate transparently with stakeholders — staff, patients, board, regulators — about the outage, the response actions taken, and the security and resilience improvements identified. Transparency builds trust; silence erodes it.



MDEXPO

ECRI ©2026 ECRI | MD Expo Baltimore

WHAT YOU CAN DO MONDAY MORNING

1. **Audit your critical device power sources** — Walk your facility and document which devices are on generator-backed circuits and which are not. This single step will reveal how much you do not know about your own infrastructure, and that knowledge gap is where the work begins.
2. **Locate or create your downtime procedures** — Find them, verify they are current, print them, and laminate them. If they do not exist, write them. Store laminated copies in known, accessible locations on each unit — not in a binder in someone's office.
3. **Build a RACI matrix for your HTM team's role** — Define who is Responsible, Accountable, Consulted, and Informed for each critical system during a digital darkness event. Share it with your IT department and your leadership team.
4. **Schedule a tabletop exercise with IT within 90 days** — Simulate a digital darkness scenario with your IT counterparts. Identify gaps in your plan, your communication, and your team's readiness. The 90-day deadline gives you accountability.
5. **Integrate digital darkness planning into your organization's overall disaster preparedness plan** — This should not be a standalone document or a one-time project. Digital darkness preparedness belongs inside your broader emergency management framework and should be reviewed alongside it.

©2026 ECRI | MD Expo Baltimore

Helpful Resources

- **Government Resources:**
- NIST Cybersecurity Framework: https://www.nist.gov/cyberframework
- FDA Medical Device Cybersecurity: https://www.fda.gov/medical-devices/cybersecurity-medical-devices
- CISA Healthcare Security: https://www.cisa.gov/healthcare-cybersecurity
- **Healthcare-Specific:**
- ECRI Cybersecurity Resources: https://www.ecri.org/solutions/cybersecurity/
- HIMSS Cybersecurity Community: https://www.himss.org/cybersecurity
- Healthcare Cybersecurity Council: https://healthsectorcouncil.org/
- **Training and Certification:**
- SANS Healthcare Security: https://www.sans.org/healthcare-security/
- ISC2 Healthcare Security: https://www.isc2.org/

MDEXPO

ECRI

©2026 ECRI | MD Expo Baltimore

ECRI | The Most Trusted Voice in Healthcare

Q&A

Jeremy Suggs, Sc.D.
Senior Engineering Manager
Device Safety
(610) 825-6000 ext. 5322
jsuggs@ecri.org



Dustin Telford AAMIF, CHTM, CBET, CRES, CLES
Associate Consultant
Healthcare Technology Consulting
(801) 879-5433
dtelford@ecri.org

MDEXPO

©2026 ECRI | MD Expo Baltimore