OVERVIEW

MEDITECH Disaster Recovery

Confidence Starts with Dependable Disaster Recovery

BENEFITS

- Increased resiliency and peace of mind for environments without existing DR.
- Lower DR infrastructure costs when augmenting current offsite configurations.
- Configurable RTO and RPO aligned with budget and recovery priorities.

WHY DRAAS FOR MEDITECH?

Many MEDITECH environments still rely on traditional, backup strategies for their on-premise environment that can fall short in a real disaster. DRaaS offers a way to strengthen your resiliency through a cloud-based solution with defined RTO and RPO goals—giving you a faster, more reliable backup and path to recovery.

- **Tailored to Your Needs:** Align Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) with your budget and operational thresholds.
- **Cloud-Ready Infrastructure:** On-premise MEDITECH environments—typically built on virtual machines and disk storage—are ideal candidates for cloud-based DR.
- **Proven in Practice:** These solutions are already trusted by some of the largest healthcare delivery networks.
- **Modernized Resilience:** Customized DR in the cloud can simplify your environment, reduce costs, accelerate deployment, and strengthen your business continuity strategy.

SHAPE YOUR DISASTER RECOVERY STRATEGY FROM WHERE YOU ARE TODAY

What are your organization's recovery expectations?

Your organization's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) define your tolerance for downtime and data loss. These metrics guide the technology requirements for your disaster recovery (DR) solution.

For example, MEDITECH MBF/ISB backups typically run once daily and are copied offsite. This strategy may support an RTO of 8–12 hours, but the RPO of 24 hours may not meet your organization's needs.

To meet your desired recovery objectives, your current data protection configurations may need to be reconfigured or augmented, depending on your risk tolerance and budget.

What virtualization platforms support your current DR plan?

Simplify your environment, stay within budget, accelerate deployment, and modernize your resiliency strategy—starting with what you already have.

Most MEDITECH sites use Nutanix-AHV, Hyper-V, or VMware. Your platform impacts your current DR capabilities and informs your next steps in the cloud journey.

- Nutanix-AHV typically replicates only to another Nutanix-AHV instance. *This limits options to:*
  - Bare Metal Cloud Nutanix
  - Traditional DR physical Nutanix sites
  - Backup/replicate/restore workflows with RPOs no lower than 12 hours
- Hyper-V and VMware, when paired with modern backup and replication tools, allow for more customization and reduced RPO/RTO—especially when recovery functions are cloud-based.

p: 855.276.9112
e: info@cerecore.net

cerecore.net

What backup software does CereCore support for DR?

CereCore supports all three MEDITECH-certified backup solutions for MBR/IDR/ISB-style backups:

- Commvault
- BridgeHead
- Networker

While all three perform backups similarly, each handles save sets and replication differently.

- On their own, each solution is limited by how often full data sets can be written locally and replicated offsite—dependent on hardware and bandwidth.
- Your hypervisor also influences which replication options are available to enhance your backup strategy.

DECISION MAKING DEEP DIVE

Some high-level questions to consider when planning your DR solution:

The best next step is to contact a CereCore representative to schedule a conversation. We'll review your current environment, desired outcomes, and help determine the best-fit strategy for your specific use case.

1. Existing Data Protection Configuration:

A. What is your current RPO/RTO?
B. What is your current backup target/method?
C. How is your offsite backup save set configured?

2. Current Infrastructure:

A. What is the current level of technical debt?
B. Are there applications that would be difficult to run in a cloud environment?
C. Has a Business Impact Analysis been conducted to prioritize recovery tiers (minimum, medium, best effort)?
D. Do you have mitigations in place for facility loss, especially for authentication (e.g., Active Directory, SAML)?

3. Network / Internet Bandwidth:

A. What is your current internet bandwidth and utilization?
B. Would your current connectivity support cloud-based system access during recovery?

These questions are starting points for assessing the readiness of your infrastructure and the strengths and weaknesses of the current disaster recovery plan.

Let's build *resiliency* and *efficiency* in your DR strategy—**contact us to get started.**

aws PARTNER Select Tier Services

CONTACT US

cerecore

cerecore.net

p: 855.276.9112 | **e:** info@cerecore.net

ABOUT US

CereCore® provides IT services that make it easier for you to focus on supporting hospital operations and transforming healthcare through technology. With a heritage rooted in our nation's top-performing hospitals, we serve as leaders and experts in technology, operations, data security, and clinical applications. We partner with clients to become an extension of the team through comprehensive IT and application support, technical professional and managed services, IT advisory services, and EHR consulting, because we know firsthand the power that integrated technology has on patient care and communities.