

CareVue Cloud

Product/Service Overview

Medsphere's CareVue Cloud option makes comprehensive EHR functionality available without the added burdens of on-premises deployment.

Via Medsphere's software-as-a-service (SaaS) strategy, the fully cloud-based version of CareVue gives customers greater accessibility and saves the expense of local servers and data centers.

CareVue and all support services run in secure and isolated Amazon Web Services' (AWS) virtual private clouds (VPCs). Each customer's private CareVue instance is replicated across two geographically separate AWS regions; CareVue resources and data are isolated from other customers and malicious intruders. CareVue applications run in the cloud and are delivered to local workstations via web browser with a small helper client.

Each client's data is separate and secure, meeting all HIPAA and HITECH requirements for security at rest and in transport. Medsphere's base Cloud offering can scale to meet the needs of any organization.

The Advantages of CareVue Cloud

Lower Capital Costs:

With CV Cloud, hospitals dispense with the need for onsite servers, hardware upgrades and specialized IT staff. Scaling up requires no additional capital investment.

IT Support Savings:

Adoption of CV Cloud means the hospital has no need to deploy desktop application suites or local data centers; maintenance of applications and servers is not required.

Peace of Mind:

Medsphere customers receive specialized and highly qualified support, standardized deployments, high availability, hourly backups and full disaster recovery systems/plans.

CareVue Cloud design is informed by lessons learned over years of on-premise CareVue deployments. Medsphere applies this knowledge to modern cloud platforms to create a solution that rivals the best on-premises deployments for a fraction of the total cost.

How CareVue Cloud Technology Works

- 1** CareVue Cloud spans multiple Amazon regions in dedicated, HIPAA-compliant, isolated virtual private clouds (VPCs).
- 2** Medsphere leverages years of CareVue systems administration expertise to enable security features that surpass HIPAA requirements and design features that exceed typical on-premise installation performance.
- 3** Each customer has a primary CareVue instance in one region and a secondary instance in a geographically distinct area, providing both high availability and disaster recovery (DR) features. This approach maximizes DR resilience during events like natural disasters that impact large geographical areas.
- 4** Included in each customer instance:
 - Complete CareVue environments
 - Load-balanced user access portal & application servers
 - 24x7 support
 - Built-in high availability & disaster recovery features
 - Off-site backups and regular backup testing
 - IPSEC VPN tunnels for secure access and transport of printer, interface, and other data between CareVue Cloud and on-premises resources

- 5** Each customer's data is encrypted in transit and at rest, and is isolated and encrypted separately from that of all other customers.

