COMMVAULT®

Best Practices for Protecting Your Epic EHR

Your Epic system is critical to not only the care you provide your patients, but to the operation of your entire organization. Protection and management of your Epic data is vital to the continuity of your business. Commvault, with input from Epic, has developed its Epic **EHR Data Protection** solution with this imperative in mind.

Commvault, drawing from its experience in protecting Epic EHR environments for numerous healthcare provider organizations, recommends that the following 10 best practices be followed to ensure the most comprehensive protection. Following these practices will help you:

- Minimize costly and disruptive system downtime
- Protect against cyber threats such as Ransomware
- Maximize system performance
- Optimize data recovery speed and data integrity

Commvault's robust EHR business continuity and disaster recovery strategies protect your clinical data, reduce risk, and help you meet EHR availability and compliance requirements

BEST PRACTICES INSERT

1 Schedule Frequent Snapshots to Minimize System Downtime
2 Encrypt All Data – Both In Motion and At Rest
3 Configure Storage Policies to Comply with Official Guidelines
4 Configure RAID Management to Minimize System Downtime, Maximize Speed
5 Back Up Your Snapshots, Even If They Are Replicated
6 Verify the Integrity of Your Data
7 Optimize Backup and Restore Processes
8 Ensure Operating System Consistency
9 Establish an Inclusive Working Group
10 Stay Current With the Most Recent Epic and InterSystems Guidelines

BEST PRACTICES

1 SCHEDULE FREQUENT SNAPSHOTS TO MINIMIZE SYSTEM DOWNTIME

The EHR is a mission-critical application, and even minimal downtime can have a significant impact on your clinical operations and, ultimately, your organization's bottom line. And in the event you need to restore this data, large gaps in data can have similar impact in terms of billing and clinical decision making.

Back up your Epic environment frequently with a snapshot-based solution. Frequent, incremental backups will minimize system downtime and minimize the window between data backups - reducing the number of journal file restores and ensuring a recent backup is always available when needed.

2 ENCRYPT ALL DATA – BOTH IN MOTION AND AT REST

Data encryption not only protects against data breaches, but also incidents like lost devices and lost backup media. Make sure your backup management solution fully supports the encryption of data both in transit and on the storage media. And be sure to configure the Caché database client to use encryption and encryption key management in accordance with industry best practices and federal regulations (HIPAA).

3 CONFIGURE STORAGE POLICIES TO COMPLY WITH OFFICIAL GUIDELINES

Make sure storage policies are configured to align with Epic guidelines. Check with Epic directly for the latest guidance, and be sure that all default values align with your Recovery Point Objective (RPO).

4 CONFIGURE RAID MANAGEMENT TO MINIMIZE SYSTEM DOWNTIME, MAXIMIZE SPEED

Cloning Epic snapshots onto a separate RAID group or array helps eliminate disruption to your Epic environment during the backup process. Both Commvault and Epic recommend full RAID clones for hard drive-based arrays that support cloning; the added redundancy and increased backup performance typically outweigh the additional storage cost. Note that RAID cloning is usually not necessary for Flash storage arrays as they typically do not suffer from the same type of I/O conflicts.

5 BACK UP YOUR SNAPSHOTS, EVEN IF THEY ARE REPLICATED

Even if you are replicating your snapshots to another array, it is still recommended that you back up your snapshots to disk, tape, or cloud. While snapshot replication is supported by Epic, it is important that your snapshots also reside in a location that does not rely on the SAN in the event of an incident that impacts SAN availability.

6 VERIFY THE INTEGRITY OF YOUR DATA

Your backup process may be working seamlessly, but this is for naught if the integrity of your restore data is compromised. Verify the integrity of this data by using the InterSystems Caché Integrity Checker utility whenever your backup configuration changes and every time you perform a test restore. At the very least, ensure you are performing these tests in accordance with Epic's recommended frequency.

7 OPTIMIZE BACKUP AND RESTORE PROCESSES

With your basic process configured, it is imperative to optimize the performance of both the backup and restore process. Your restores will never be faster than your backups; keeping the gap between these two processes as slim as possible is critical should you need to execute a restore. Follow these steps to put yourself in the best position:

- Use multiple data readers to back up your InterSystems Caché databases
- Run complete, daily backups on your InterSystems Caché database sub client. If this backup does not complete within 24 hours, optimize/upgrade your backup infrastructure.
- Make sure your backup software is able to restore data from multiple streams via magnetic library or tape copy. The number of streams used for backup must match the number of streams for restore to ensure the fastest restores possible in the case of a disaster

Commvault Data Protection for Epic's Caché Database

Discover how Commvault software seamlessly captures, protects, and backs-up the entire Epic Caché database.

READ NOW

PDF

commvau.lt/2orsPHB

The amount of data you manage grows every day, and the technology you use for this management is always trending towards obsolescence. Monitor the performance of your backup and restore processes regularly to ensure that the parameters set by Epic, InterSystems, your backup vendor, and your organization are being met. Anticipate upgrades and reconfiguration – particularly during the budgeting process – and reduce infrastructure upgrade "fire drills" by having a plan in place to deal with upgrades.

8 ENSURE OPERATING SYSTEM CONSISTENCY

Using different operating systems for your production Caché server and your backup proxy server can cause incompatibilities in file systems and volume structures. Play it safe; use the same operating system for both of these systems.

9 ESTABLISH AN INCLUSIVE WORKING GROUP

Successful data protection and management requires collaboration from a number of different individuals. The stakes are high; it is imperative that you create a team that works together to ensure success. Your Caché database administrators, backup administrators, and infrastructure managers should all be part of this working group. Meet regularly and with purpose.

10 STAY CURRENT WITH ALL CURRENT EPIC AND INTERSYSTEMS GUIDELINES

Underlying all of these best practices is the need to stay current with all guidelines and recommendations put forward by Epic, InterSystems, and your backup software vendor. Your working group should make reviewing and implementing any updates part of their team agenda. Here are some resources that should be referenced regularly:

- InterSystems Caché Data Integrity Guide
- For Commvault customers: Epic Solution Best Practices
- Epic Business Continuity Technical Solutions Guide

▶ Commvault, a leader in data backup and recovery, has developed its EHR Data Protection solution with direct input from Epic. The solution is currently used to protect critical Epic environments for a number of healthcare provider clients. **More information about this solution can be found at commvault.com/healthcare.**