dbtech

EBOOK

Features a Downtime Solution Needs

Table of Contents

The market for EHR downtime solutions has matured significantly over the past decade. Almost every major vendor now claims to offer a downtime solution, and the sales pitches can start to sound identical. Seamless integration. Real-time data. Easy implementation. Automatic recovery.

The reality is that downtime solutions vary enormously in their capabilities, their integration depth, and their actual performance when a real outage occurs at 2:00 AM. The features that separate adequate solutions from genuinely effective ones are specific, technical, and often not visible in a standard product demo.

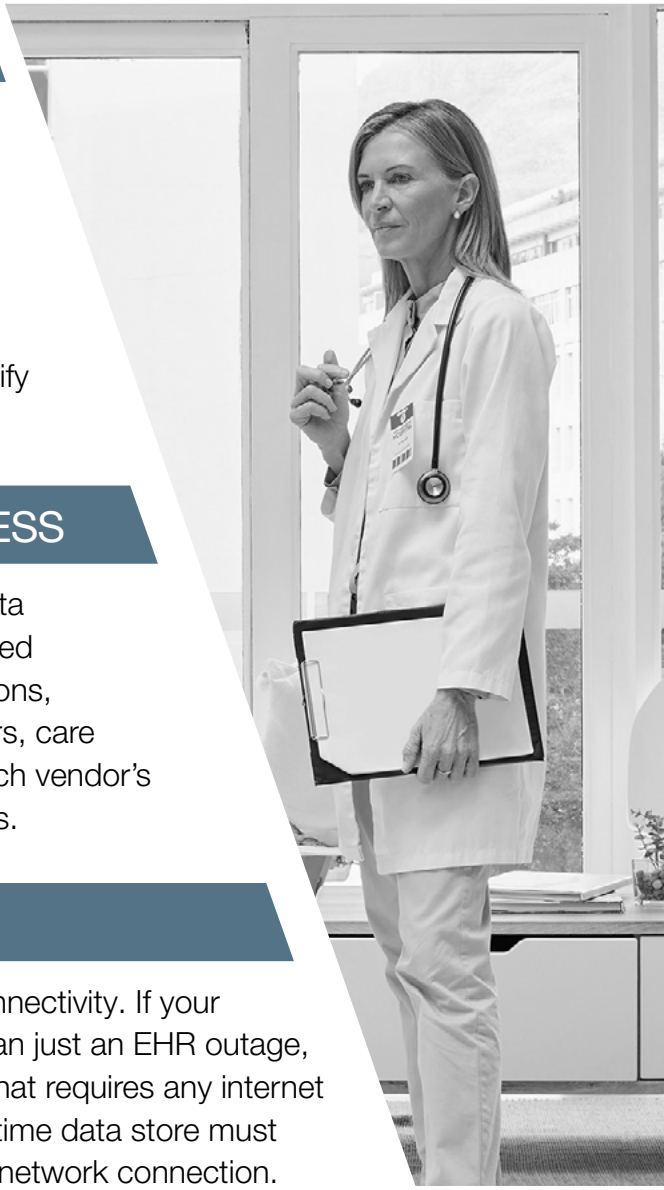
This guide gives healthcare IT and operations leaders a comprehensive feature checklist to evaluate any downtime solution on the market. It covers must-have core capabilities, integration requirements, security and compliance standards, and operational considerations that vendors often gloss over.

Core Data Capabilities

The fundamental job of a downtime solution is to give clinicians access to accurate patient data when the EHR is unavailable. How that data is captured, stored, and presented determines whether the solution actually works in a crisis.

REAL-TIME DATA SYNCHRONIZATION

The solution must sync continuously with your EHR, not on a nightly batch or hourly schedule, but in real time. Patient records updated in the EHR five minutes before a downtime event must be available in the downtime system immediately. Any gap in synchronization means clinicians are working with stale data, which introduces clinical risk. Ask vendors to specify the exact synchronization frequency and demonstrate it.



COMPREHENSIVE PATIENT RECORD ACCESS

A downtime solution that only provides demographic data is not a downtime solution, it is a directory. Clinicians need access to the complete patient record: current medications, allergies, active problem lists, recent labs, pending orders, care team assignments, and advance directives. Evaluate each vendor's data depth against your facility's actual clinical workflows.

OFFLINE-FIRST ARCHITECTURE

The solution must operate independently of network connectivity. If your downtime event is caused by a network failure rather than just an EHR outage, which is common in ransomware scenarios, a solution that requires any internet or intranet connectivity to function is useless. The downtime data store must be local, self-contained, and fully functional without any network connection.

KEY QUESTIONS TO ASK VENDORS

- What is the exact real-time sync interval? How is this verified?
- What percentage of the patient record is available during downtime?
- Can the solution function with zero network connectivity?
- How is data stored locally, encrypted database, file system, other?
- What is the maximum patient census supported at full data depth?

EHR Integration and Recovery

Integration is where most downtime solutions either prove their value or reveal their limitations. The ability to connect with your specific EHR platform, and to automatically reconcile downtime data when systems recover, determines the total cost and operational burden of any downtime event.

NATIVE EHR INTEGRATION VIA HL7

The gold standard for downtime solution integration is native HL7 interface support, not screen scraping, not API workarounds, but real HL7 messaging that treats the downtime system as a proper node in your healthcare data exchange. This enables automated data flow in both directions: pulling current data into the downtime system before an outage, and pushing downtime registration data back into the EHR during recovery.

MULTI-EHR AND LEGACY SYSTEM SUPPORT

Healthcare organizations rarely run a single EHR. Satellite facilities, acquired practices, and legacy departmental systems create complex data environments. Evaluate whether the downtime solution can integrate with all relevant systems in your environment, not just your primary EHR. Vendors with proven integration tracks across Epic, Cerner, MEDITECH, and Lawson/Infor are significantly lower risk than single-platform specialists.

AUTOMATED POST-DOWNTIME RECONCILIATION

Manual re-entry of downtime data into the EHR is the single largest source of hidden downtime cost. The solution must be capable of automatic reconciliation, using HL7 messages to update EHR records with data captured during the downtime period, without requiring staff to re-key any information. This feature alone can justify the cost of a premium solution.

Security, Compliance, and Reliability

A downtime solution that creates security vulnerabilities or compliance gaps is worse than no solution at all. Evaluate every vendor rigorously against these requirements.

HIPAA-COMPLIANT DATA HANDLING

All patient data stored in the downtime solution must meet HIPAA technical safeguard requirements: encryption at rest and in transit, access controls with audit logging, automatic session timeout, and breach notification support. Request a copy of the vendor's HIPAA compliance documentation and Business Associate Agreement before advancing any vendor to finalist stage.

ROLE-BASED ACCESS CONTROLS

Not every staff member needs access to every patient's complete record. The solution must support granular role-based permissions that mirror your EHR access control model. Unit-specific access, function-based restrictions (registration staff vs. clinical staff), and emergency override protocols with audit trails are all essential.

RELIABILITY AND UPTIME STANDARDS

Evaluate vendors on these reliability indicators:

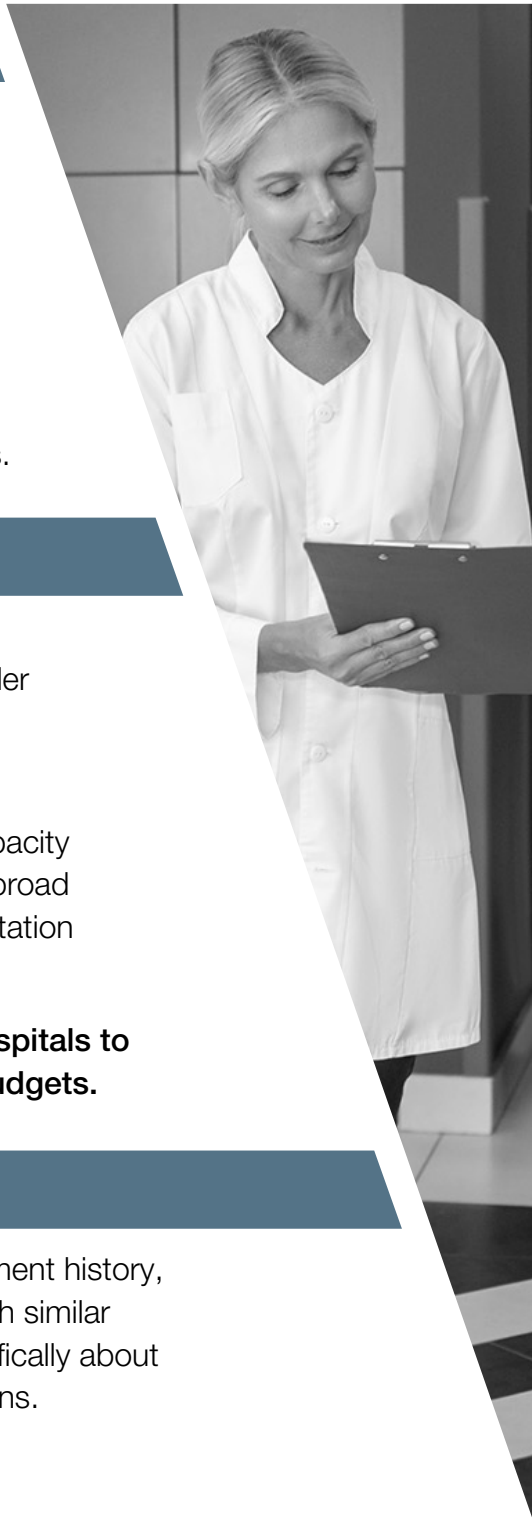
- SLA guaranteed uptime for the downtime system itself (target: 99.9%+)
- Redundant data storage to prevent the downtime solution from becoming a single point of failure
- Tested disaster recovery procedures with documented RTO and RPO
- Regular data integrity verification between the downtime system and the EHR
- 24/7 vendor support with documented response time SLAs

Operational Considerations

IMPLEMENTATION AND TRAINING

The best featured solution is worthless if staff cannot use it under pressure. Evaluate the vendor's implementation methodology, training approach, and ongoing support model carefully.

Effective downtime training is scenario-based and regularly refreshed. Staff who practiced downtime procedures six months ago and have never used them in a real event will struggle when an actual outage occurs. Look for vendors who provide training materials, simulation tools, and support for regular downtime drills.



SCALABILITY AND PRICING MODELS

Downtime preparedness should be accessible to organizations of all sizes. Tiered pricing models based on station count allow smaller facilities and critical access hospitals to deploy a real downtime solution within budget constraints, then scale as they grow.

Be cautious of flat enterprise pricing that forces you to pay for capacity you do not need, or per-user models that create disincentives to broad deployment. The goal is to have downtime access at every workstation that needs it, not to manage a limited seat count during a crisis.

Tiered pricing based on station count enables critical access hospitals to deploy genuine downtime protection without enterprise-scale budgets.

VENDOR TRACK RECORD

Downtime solutions should be evaluated based on actual deployment history, not marketing materials. Ask for references from organizations with similar size, EHR platforms, and downtime scenarios to yours. Ask specifically about experiences during actual outage events, not just routine operations.

- How many facilities does the vendor support?
- What is the average tenure of current customers?
- Has the vendor supported a customer through a major ransomware event?
- What is the vendor's own uptime history over the past 24 months?
- What is the average implementation timeline from contract to go-live?

The Complete Evaluation Scorecard

Use this scorecard when evaluating vendors. Score each feature from 1 (not present) to 5 (fully demonstrated with references).

#	Feature	Score (1–5)
01	Real-Time Data Synchronization	/5
02	Comprehensive Patient Record Access	/5
03	Offline-First Architecture	/5
04	Full Patient Registration During Downtime[1.1][2.1]	/5
05	Wristband, Label, and Form Printing	/5
06	Electronic Forms and eSignature	/5
07	Dynamic and Customizable Forms	/5
08	Native EHR Integration via HL7	/5
09	Automated Post-Downtime Reconciliation	/5
10	Multi-EHR and Legacy System Support	/5
11	HIPAA-Compliant Data Handling	/5
12	Role-Based Access Controls	/5
	Total	**/60**

A vendor scoring below 4 on any must-have feature (01–06, 08–09, 11–12) should be disqualified. A combined score below 50 out of 60 suggests meaningful capability gaps that will surface during an actual downtime event.

Conclusion: The Right Solution Performs When It Matters Most

The purpose of a downtime solution is not to check a compliance box or satisfy an accreditation surveyor. It is to protect patients and staff during one of the most stressful operational scenarios a healthcare facility can face. The solution you choose will be called upon during a network failure, a ransomware attack, or a catastrophic system crash. It needs to work.

The 12 features in this guide are not a wish list, they are the baseline for a solution that will actually perform under real-world conditions. Use this framework to cut through vendor marketing, ask the right questions, and make a procurement decision that you can defend to your board, your clinical leadership, and your patients.

dbtech has been delivering a downtime solution to healthcare organizations since 1983 w with Epic, Cerner, MEDITECH, and Lawson/Infor, we offer the experience and the technical depth to deliver on every capability in this guide.

See how dbtech scores on all 12 features. Request a demo
and walk through the scorecard with a dbtech consultant.

 dbtech.com

 (732) 638-0893

 info@dbtech.com