Proceedings of Business and Economic Studies, 2026, Volume 9, Issue 8
http://ojs.bbwpublisher.com/index.php/PBES
Online ISSN: 2209-265X
Print ISSN: 2209-2641

Discussion on Difficulties and Improvement Measures of Information Network Operation and Maintenance Management in Digital Hospital Construction

Dushu Cai[1], Jianghong Tang[1], Dechong Yu[2], Zhangxing Chen[1]*

[1]Information Center, The Second Affiliated Hospital of Wenzhou Medical University, Wenzhou, Zhejiang, China
[2]Logistics Support Office, Longgang Campus, The First Affiliated Hospital of Wenzhou Medical University, Wenzhou, Zhejiang, China

Author to whom correspondence should be addressed.

Abstract: With the deepening of medical information construction, the information network has become the core infrastructure to support the operation of hospital clinical business. However, the complexity of the system continues to rise, the risk of downtime is increasing, the data island is still stubborn, the network security threat is upgraded, and the shortage of compound talents; these factors have brought severe challenges to the hospital information network operation and maintenance management. This study systematically sorted out the core difficulties of digital hospital network operation and maintenance from three dimensions of technology, organization, and management, and put forward a set of systematic improvement paths, such as building a high-availability architecture and emergency response system, promoting interoperability standardization, introducing intelligent operation and maintenance tools, and establishing a data-driven organizational governance mechanism. The research points out that only by relying on the two-wheel drive of technology and organization can it transform the operation and maintenance department from the traditional cost center to the strategic support force in the digital transformation of the hospital.

Keywords: Digital hospital; Information network; Operation and maintenance management; System downtime; Interoperability

---

Online publication: August 31, 2026

1. Introduction

The wide application of electronic medical records, Internet of Things medical equipment, telemedicine, and other technologies is profoundly reshaping the business form of modern hospitals [1]. The hospital information system has also gradually evolved from an auxiliary tool in the past to an indispensable central nervous system in clinical business operations. According to relevant statistics, a large tertiary hospital's daily business system operations can reach dozens of sets, more than ten thousand network terminals, and system interface calls daily are millions of times [2].

However, the deepening of digitization has not brought about a linear improvement in operation and maintenance capabilities [3]. The more complex the system is, the more vulnerabilities it exposes. The deeper the business depends on the information system, the heavier the cost of downtime. And such failures are mostly concentrated in the peak hours of clinical business [4]. This finding actually reveals the fundamental contradiction faced by the current operation and maintenance work: that is, the high dependence of clinical business on digital systems and the tension between the uncertainty of traditional operation and maintenance models in complex environments. This paper aims to systematically identify the key difficulties, learn from international experience, and then sort out an operable improvement path.

2. Main difficulties of network operation and maintenance management in digital hospital

2.1. System complexity and downtime risk

The modern hospital network covers dozens of heterogeneous systems such as HIS, EMR, PACS, LIS, surgical anesthesia, intensive care, etc. These systems are provided by different manufacturers. The technical architecture and interface protocols are different, and there are a lot of dependencies between them [5]. This highly coupled architecture will bring double problems: First, any subsystem upgrade or configuration adjustment may trigger a chain reaction through the interface and spread to other modules, which makes change management extremely complex; second, it is difficult to trace the fault, and it takes a long time to troubleshoot.

The clinical consequences caused by the system downtime are particularly serious. During the downtime, doctors cannot access the patient's historical medical records and allergy history. Pharmacists cannot check the prescription, and the test results cannot be returned in time. Fang *et al.*'s research found that unplanned downtime accounts for up to 96.1% and is concentrated in the working day and morning hours, which happens to be the busiest time for clinical business; the complexity of the system itself makes it difficult to predict the recovery time, which brings huge technical challenges to the operation and maintenance team [6].

2.2. Interoperability deficiencies and data silos

Because the business systems are built in stages and the manufacturers are different, most of the early online systems adopt private data formats and proprietary interfaces. Even if the new system later declares that it supports standards such as HL7 FHIR, when it comes to the actual landing link, it still cannot bypass the practical problems such as "inconsistent implementation of manufacturers." In order to achieve interconnection, it is still inseparable from a large amount of customized development [7].

The obstacles fall not only on the technical level, but also on the governance level. Sustainable medical information exchange needs to be promoted from the four dimensions of governance mechanism, enterprise architecture, talent ability, and standard adoption. In the practice of county hospitals in China, the phenomenon of low integration of multi-supplier systems and "information islands" will be particularly prominent. In addition, the data collection path and statistical caliber are not uniform, which seriously restricts the full release of data value.

2.3. Network security threats and compliance pressure

With its high sensitivity, medical data has become the target of ransomware and APT attacks. At the same time, the regulatory requirements of various countries have become more and more stringent. From the EU GDPR, German IT Security Act 2.0 to China's data security law and equal protection requirements, there is a mandatory compliance pressure on hospitals [8]. The long-term lack of security investment, coupled with the irreconcilable contradiction between security and efficiency, has made hospital network security fall into the dilemma of "high value and low protection." For small and medium-sized hospitals, it is a very heavy burden to build a complete three-level safety system, whether in terms of capital or manpower.

2.4. Talent shortage and skill mismatch

The operation and maintenance of digital hospitals has a high demand for compound talents. It is necessary to have knowledge of network engineering, information security, database management, and medical business processes at the same time. However, such compound talents are very scarce. County hospitals are faced with two dilemmas: on the one hand, the information department lacks the technical reserves to maintain complex systems; on the other hand, the business department lacks the ability to apply data analysis tools. The lack of technical capabilities has caused excessive reliance on external suppliers, and the time for fault response has therefore been prolonged. Mohammadi and Ahmadi also mentioned that the lack of awareness of digital values by management and medical staff will also pose a major obstacle. Under the superposition of these factors, IT departments often fall into a vicious circle of "insufficient capacity → not being valued → less resources." See **Table 1**.

Table 1. Mechanism of talent shortage and vicious cycle in digital hospital operation and maintenance at county-level hospitals

Dimension	Core contradiction / specific manifestations
High demand for compound talents	Requires simultaneous expertise in: Network Engineering + Information Security + Database Management + Medical Business Processes
Low supply in county-level hospitals	IT Department: Lacks technical reserves for maintaining complex systems; Business Department: Lacks capability in applying data analysis tools
Intermediate outcome	Excessive reliance on external suppliers → Prolonged fault response time
Vicious cycle closure	Insufficient capacity → Not being valued → Reduced resource allocation → Further capacity decline

3. Improvement measures of network operation and maintenance management in digital hospital

3.1. Building high availability architecture and emergency response system

To deal with the risk of downtime, it is necessary to implement redundant design at the architecture level and establish a hierarchical response mechanism at the emergency level [9].

At the architecture level, the core system needs to adopt cluster deployment, load balancing, and database master-slave hot standby. For key systems such as EMR, a read-write separation mechanism can be introduced to divert query operations to read-only copies. In this way, even if the main library is in the maintenance period, the clinical end can still access historical data. The practice at Severance Hospital in South Korea provides a valuable reference: they ensure data availability by switching to a read-only backup server during planned downtime; at the same time, an emergency prescription system independent of the main HIS was developed based on Microsoft Power Platform, and 22 prescriptions were successfully issued within a 90-minute shutdown window. The core implication is that the emergency system is not simply to return to the paper process, but to retain the digital capabilities as much as possible within the scope of technology. See **Figure 1**.

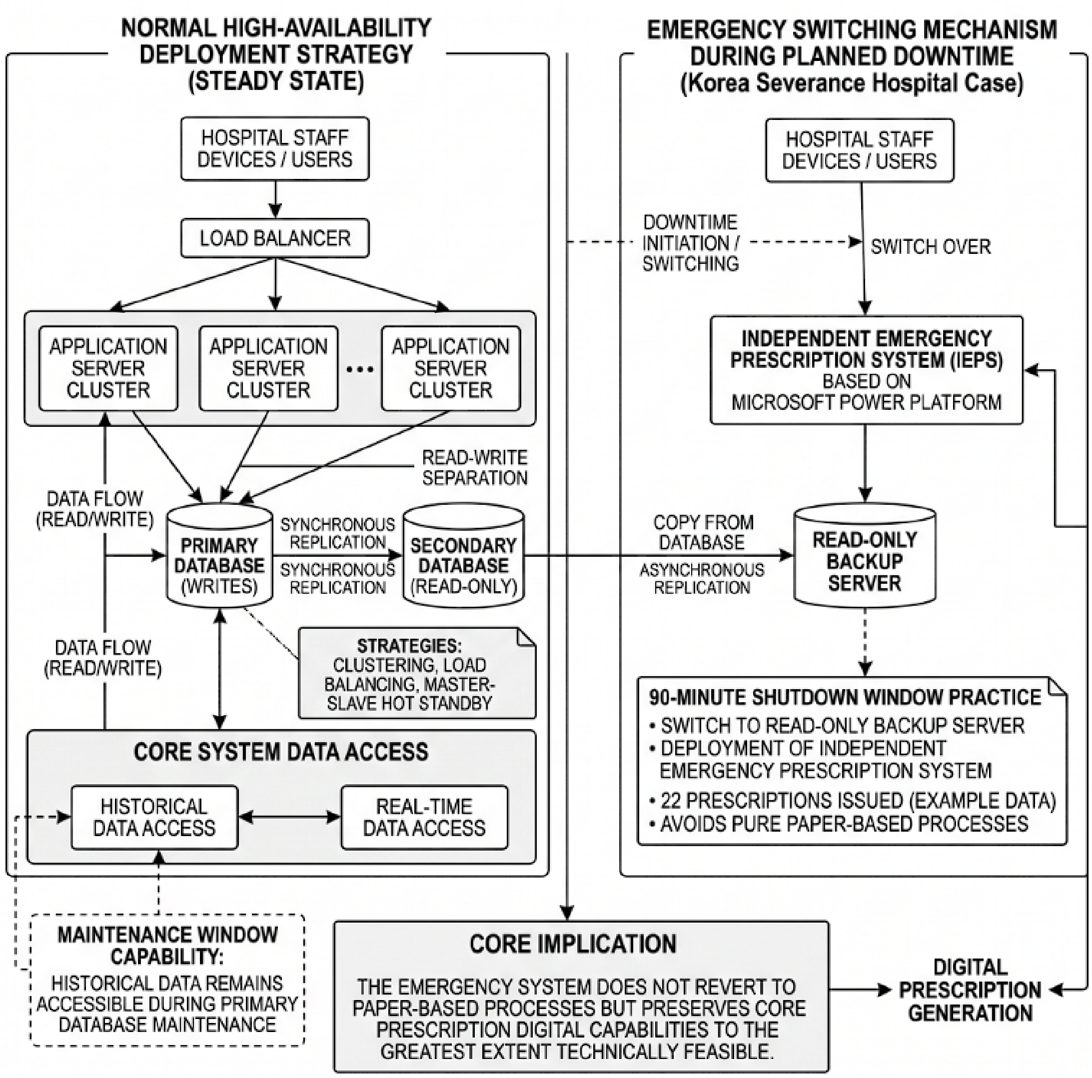

Figure 1. Dual-track operation mechanism of high-availability architecture and emergency prescription system in digital hospitals

At the institutional level, the US SAFER guidelines provide a framework for downtime management covering four stages of prevention, preparation, response, and recovery, including standby paper forms, downtime drills, and patient identification specifications. Based on this, hospitals should formulate hierarchical emergency plans and transform the emergency response model from post-event decision-making to a standardized process that has been rehearsed in advance. Ultimately, institutionalizing this proactive, process-driven downtime management approach in hospitals—based on a mature framework such as the US SAFER Guidelines—can significantly improve patient safety in the face of inevitable interruptions in the system, ensure the continuity of clinical business, and maintain the organization's ability to resist risks.

3.2. Promoting standardized interoperability and open system selection

To solve the data island, it is necessary to promote the coordination of technical standards and governance mechanisms. Technical standardization ensures seamless interoperability across heterogeneous systems by unifying data formats, interfaces, and communication protocols, thereby eliminating barriers to data flow.

At the technical level, it is necessary for hospitals to consider standardized interoperability as a rigid indicator in the system procurement stage. The German ISiK initiative defines a unified API based on HL7 FHIR, so that new applications can complete standardized communication with HIS of different manufacturers. Chinese hospitals should also actively promote the adoption of international standards such as FHIR and DICOMweb to prevent the construction of new "standard chimneys" [10]. This strategic change requires that in the procurement contract, it must be clearly agreed that these standards must be met, and those proprietary interfaces that deeply bind the hospital to a single supplier ecology must no longer be accepted; at the same time, a phased migration roadmap should be developed to prioritize high-frequency data exchange scenarios such as images and test results. By embedding interoperability requirements into the system procurement process as soon as possible, hospitals can gradually dismantle existing data silos and ensure that newly invested resources serve the long-term goal of seamless data flow throughout the hospital, rather than in turn exacerbating fragmentation. See **Figure 2**.

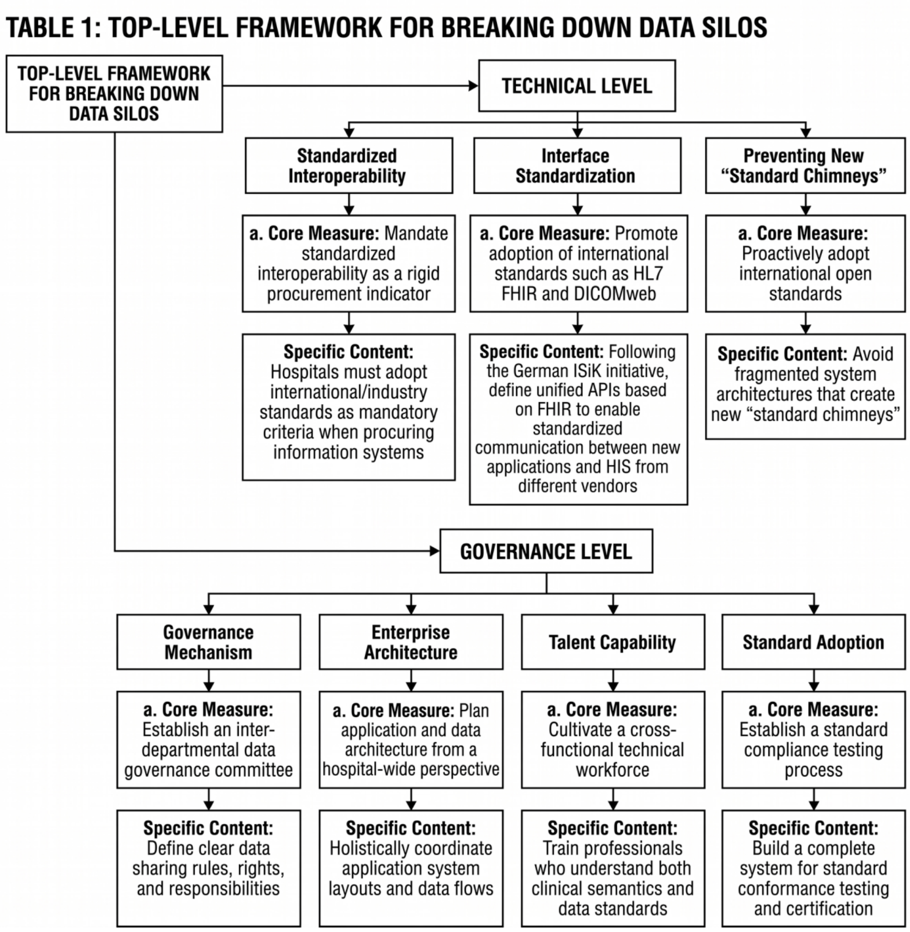

Figure 2. Top-level framework for breaking down data silos

At the governance level, the "Mind the GAPS" framework clearly states that the construction of interoperability needs to be promoted from four dimensions: first, the governance mechanism, which should establish an inter-departmental data governance committee and formulate clear data sharing rules; the second is the enterprise architecture, which must plan the application and data architecture from the perspective of the whole hospital; the third is the ability of talents. It is necessary to train a group of technicians who understand both clinical semantics and data standards. Fourth, standard adoption should establish a set of standard compliance test processes. These four dimensions are indispensable. The reason why many interoperability projects fail is that they only focus on technical standards and ignore governance construction.

3.3. Introducing intelligent operation and maintenance and automation management tools

The reason why AI-driven network management tools can achieve significant cost reduction and efficiency increase is that it transforms the operation and maintenance activities that rely on manual experience judgment into a data-driven automated decision-making process, which is embodied in the following four aspects: First, the automatic topology discovery function, which can draw the network device connection diagram in real time, dynamically perceive the change of the network structure, thus overcoming the common lag and error of manual drawing topology diagram; the second is the real-time performance monitoring and abnormal early warning module. By collecting key indicators such as bandwidth utilization, delay, and packet loss rate, and using machine learning algorithms to establish a dynamic baseline, it can identify potential risks and trigger warnings before the failure occurs, thereby converting passive emergency response to active prevention; the third is the capacity prediction function, which predicts the bottleneck of network resources based on the trend analysis of historical data, provides a scientific basis for capacity expansion planning, and avoids business interruption caused by insufficient resources. The fourth is automated patch management, which can regularly scan device firmware and system vulnerabilities, and automatically complete patch updates according to the preset strategy, which greatly shortens the security window period.

The synergy of the above capabilities not only enables network operation and maintenance to move from "fire-fighting" passive response to "predictive" active governance, but also fundamentally reduces the probability of human error and provides a reliable guarantee for the stable operation of large-scale networks.

In the frontier direction, the "clinical intent translation network" framework based on the large language model allows the operation and maintenance personnel to describe the business requirements in natural language, and the system automatically parses the intent, generates the network strategy, and performs security verification. The experimental results show that the network reconfiguration time in emergency scenarios has been significantly shortened. Although it is still at the forefront of research, its path is very clear: AI technology is expected to greatly lower the technical threshold of network operation and maintenance, thus alleviating the dilemma of talent shortage.

3.4. Establishing a data-driven organizational governance and talent training mechanism

The improvement of the technical level is inseparable from the supporting support at the organizational level. Taking the evaluation of "digital coordination centers" as an example, strong leadership support, clear division of responsibilities, and the integration of IT into clinical governance structures have proven to be key enablers for the success of digital projects.

In terms of personnel training, county hospitals should take the road of combining "bringing in" and "going out." They should not only establish a cooperative training relationship with universities and information centers of the top three hospitals, but also open up channels for internal employees to continue to improve. At the same time, the coverage of training must also be extended to the data literacy of clinical medical staff, because this is an important prerequisite for digital tools to truly exert clinical value. It is particularly critical that the coverage of training must go far beyond the information technology department and include the data literacy of clinical medical staff. This is an extremely important but often overlooked dimension, because the clinical value that digital tools can ultimately play—whether it is electronic health records, clinical decision support systems, or artificial intelligence-assisted diagnostic aids—does not depend on the complexity of the technology itself, but on the ability of front-line clinicians to effectively interpret the data generated by these tools, build trust, and take action accordingly. If a surgeon cannot critically evaluate the output of the prediction algorithm, or a primary care physician lacks the skills to query the data dashboard to obtain actionable patient insights, it will become an insurmountable bottleneck for any technology investment.

4. Conclusion

The functional orientation of the network operation and maintenance of the digital hospital is no longer limited to the traditional "ensuring no downtime," but has begun to shift to the comprehensive function of "supporting clinical continuity, ensuring safety compliance, and driving refined management." To cope with this transformation, on the one hand, it is necessary to build a high-availability architecture at the technical level, promote standardized interoperability, and deploy intelligent operation and maintenance tools; on the other hand, it is also necessary to improve the governance mechanism, cultivate compound talents, and reengineer the management process at the organizational level. Only by relying on the two-wheel drive of technology and organization can the operation and maintenance department be transformed from the traditional cost center into a strategic support force for the digital transformation of the hospital. No matter how the technology changes, the principle of "patient safety as the center and clinical value as the guidance" should always fall at the root of hospital network operation and maintenance management.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Shaw L, Senthilkumar V, Smith A, 2025, Digital Coordination Centres in Australian Hospitals: Implementation Challenges and Enablers. BMC Health Services Research, 25(1): 421–435.

[2] Adoption Frameworks for Digital Health Solutions in Hospital Settings, 2026, In: Digital Health Transformation: From Strategy to Operations, 87–124, Springer, Singapore.

[3] Wang H, Zhang L, Chen Y, 2026, Clinical Intent-Based Networking Automation: A Large-Language-Model-Enhanced Framework for Healthcare Infrastructure Management. IEEE Internet of Things Journal, 13(9): 18154–18166.

[4] Sittig DF, Singh H, Classen DC, 2025, SAFER (Safety Assurance Factors for EHR Resilience) Guide Recommended Practices for Managing Electronic Health Record Downtime. Journal of the American Medical Informatics Association, 32(4): 712–720.

[5] NHS England Digital, 2024, Smart Network Management Report: Automation and AI-Driven Operations in Healthcare IT (Report No. NHS-DIG-2024-037), London: NHS England, 1–58.

[6] Zhou S, Yin H, 2026, Navigating Challenges and Opportunities: A SWOT Analysis of Digital Management Center Implementation in County Hospitals. Frontiers in Public Health, 14: 1456789.

[7] Fang Q, Li J, Wu Z, 2025, Electronic Health Record Downtime Events of a Hospital: A Retrospective Analysis from Adverse Event Reports. Applied Clinical Informatics, 16(5): 1419–1429.

[8] Park S, Kim J, Lee H, 2024, Strategy for Scheduled Downtime of Hospital Information System Utilizing Third-Party Applications. BMC Medical Informatics and Decision Making, 24: 300–312.

[9] Marcelo A, de Lusignan S, 2026, AeHIN Framework for Regional Health Information Systems Interoperability. In: Digital Health in Asia: Policy, Implementation and Governance, 201–228, Elsevier, Amsterdam.

[10] Mohammadi R, Ahmadi M, 2025, Challenges of Establishing a Smart Hospital in Taft City in 2025: A Qualitative Study. Journal of Health Management & Information Science, 12(3): 189–198.