Digital Saturation and Health System Collapse: Toward Resilient Design of Information Systems in Complex Care Environments

Roozbeh Hojabri[1], Mahmoud Manafi[2]

[1] Manafi Institute for Saturation Studies (MISS), Researcher, hojabri@manafi-institute.de

[2] Manafi Institute for Saturation Studies (MISS), Researcher, manafi@manafi-institute.de

Abstract

Digital and information systems have become integral to healthcare delivery, enhancing efficiency, coordination, and access to services. However, increasing reliance on these systems may also introduce new forms of systemic vulnerability. This study examines how digital systems contribute to service disruption and explores the concept of digital saturation through the lens of the Stability–Efficiency–Adaptability (SEA) model.

A qualitative design was employed, combining a structured review of disruption factors with semi-structured interviews conducted with 13 participants across clinical, technical, and managerial domains. The analysis was guided by key disruption factors, including technical failures, cybersecurity threats, infrastructure dependency, workflow over-integration, loss of reversibility, and AI-related limitations.

The findings reveal that healthcare systems are increasingly optimized for efficiency, often at the expense of stability and adaptability. High levels of digital dependency, combined with limited manual fallback capacity, make systems highly sensitive to disruption. Failures such as downtime, connectivity issues, and cyber incidents were found to rapidly affect service continuity and, in some cases, propagate across interconnected systems.

Interpreted through the SEA model, these findings suggest that efficiency-driven digital transformation may lead to reduced adaptability and increased fragility, resulting in a condition of digital saturation. The study highlights the need for resilience-oriented design approaches that restore balance among stability, efficiency, and adaptability to ensure reliable healthcare delivery.

Keyword: Digital Saturation, Information Systems, Health System Collapse, Digital Health, Failure, Healthcare Systems, SEA Model, AI

1. Introduction

Health systems are increasingly shaped by digital transformation through the expansion of electronic health records (EHRs), digital imaging and laboratory systems, artificial intelligence (AI), and telemedicine infrastructures, largely because these technologies are expected to improve clinical quality, cost-efficiency, coordination, and access to care (Abed et al., 2024; Larsen et al., 2019). In rural and distance areas, this promise is especially important, since telehealth and related digital services are often positioned as mechanisms for extending care where geography, staffing, and service availability create persistent barriers (Hojabri et al,2012; Fontalvo et al., 2025; Hojabri & Manafi, 2025a).

At the same time, the same literature shows that digital transformation also creates forms of digital dependence. The WHO report on cyber-attacks in health care explicitly notes that while digital transformation improves safety and efficiency, it also creates dependence that can be exploited through ransomware and other attacks on healthcare delivery systems (WHO, 2024; Abed et al., 2024). Research on EHR downtime similarly shows that when core systems become unavailable, patient care processes are disrupted, safety mechanisms such as clinical decision support are deactivated, and patient safety may be compromised (Larsen et al., 2019). Evidence from hospital cyberattack cases further shows that when digital systems are tightly integrated across clinical, administrative, logistical, and communication layers, the disruption does not remain local; it can affect the whole organization and require prolonged recovery (Abbou et al., 2024).

These concerns become sharper when viewed through the concept of digital saturation. Klein and Manafi (2026) argue that saturation emerges when technological acceleration outpaces human, institutional, and structural capacity for adaptation, producing recursive dysfunction, rigidity, and breakdown rather than sustained progress. This broader saturation logic is consistent with Manafi's (2025) theory of saturation, which treats crises and collapse not as isolated events but as the cumulative result of overload, compressed feedback, and declining adaptive capacity. In health systems research, the same concern appears in work showing that persistent optimization and efficiency pressure can erode buffers, reduce flexibility, and gradually push systems toward saturation and functional breakdown (Hojabri & Manafi, 2026 a,b).

The problem is not limited to outages or cyberattacks. Studies of health information technology show that IT problems can disrupt care delivery, propagate information errors, and in some cases harm patients, while current reporting often fails to capture these effects in a sufficiently structured way (Kim et al., 2017). AI introduces a related challenge: performance in testing does not guarantee safe or equitable performance in real-world deployment, especially when the deployment population differs from the training or validation environment, creating risks of deterioration, false alarms, missed cases, and biased clinical decisions (Cross et al., 2024). Telemedicine is also not universally resilient; evidence suggests that where rural digital infrastructure is weak, telehealth investments may yield limited benefit, and meaningful effects only emerge after minimum infrastructure thresholds are reached (Fontalvo et al., 2025). From a system perspective, these disruptions matter because health system collapse is increasingly understood as a progressive, saturation-driven process rather than a single catastrophic event (Hojabri & Manafi, 2026 b). The SEA model is useful here because it interprets collapse as the result of prolonged imbalance among stability, efficiency, and adaptability, with excessive efficiency orientation weakening adaptive capacity and increasing systemic fragility (Hojabri & Manafi, 2026 b). Hojabri and Manafi (2026 b) developed an early warning framework, also identifies digital and information system failure as one of the seven core factors of healthcare system collapse and links it to the use of data for reporting and control rather than for learning and adaptation.

Against this background, this study aims to examine how digital dependency can become a pathway to service disruption and broader system vulnerability in healthcare. It argues that digital systems should be understood not only as enablers of performance, but also as infrastructures that may amplify risk when redundancy, fallback capacity, infrastructure resilience, contextual fit, and long-term support are inadequately designed. By centering digital saturation and interpreting the findings through the SEA model, the study seeks to contribute to Information Systems research by shifting attention from digital adoption alone toward the resilient design conditions required to prevent temporary service collapse, erosion of trust, and deeper systemic instability.

2. Literature review

Digital transformation has become a defining feature of contemporary health systems, particularly through the expansion of electronic health records (EHRs), hospital information systems, telemedicine, artificial intelligence (AI), and digitally mediated care infrastructures. Across the uploaded literature, these technologies are consistently presented as mechanisms for improving efficiency, service coordination, clinical decision-making, and access to care, especially in underserved or geographically remote settings (Hojabri & Manafi, 2026 a; Larsen et al., 2019; Maita et al., 2024; Tilhou et al., 2023). At the same time, the reviewed evidence shows that digital transformation also produces a new structural condition: deep dependency on digital infrastructures for routine service continuity. The WHO report on cyber-attacks explicitly states that the replacement of paper-based processes with digital alternatives improves quality and efficiency but simultaneously creates digital dependence that can be exploited through cyber threats against health-care delivery systems (WHO, 2024; Abed et al., 2024). The same dependence is visible in hospital level downtime studies, where the unavailability of EHRs immediately affects care coordination, laboratory reporting, documentation quality, and patient safety (Larsen et al., 2019; Larsen et al., 2017).

A central cluster of reviewed studies concerns EHR/HIS downtime and operational fragility. Larsen et al. (2019) show that EHR downtime is operationally disruptive and delays laboratory result reporting, while also making data capture more difficult precisely at the moment when system performance should be most visible. Larsen et al. (2017) further demonstrate that downtime-related patient safety events are concentrated around laboratory processes, medication ordering, patient identification, and communication of clinical information, and that downtime procedures are often either absent or poorly followed. Lyon et al. (2023) and Jo et al. (2024) extend this by showing that continuity during downtime requires not only backup technologies but also prior preparation, user education, mock drills, emergency viewers, emergency prescription pathways, and organizational coordination; in other words, resilience must be designed and rehearsed rather than assumed.

A second major cluster of evidence concerns cybersecurity, ransomware, and digitally induced service breakdown. Abbou et al. (2024) document that a major cyberattack can shut down all hospital computer systems and disrupt clinical work across the organization, showing that digital failures are not limited to administrative inconvenience but can affect the continuity of care itself. Neprash et al. (2022) show that ransomware attacks on U.S. health care delivery organizations more than doubled over the study period and that a large share of attacks disrupted care delivery through downtime, cancelled services, and ambulance diversion. Additional reviewed evidence suggests that these disruptions may also spill beyond the targeted organization, affecting nearby hospitals and redistributing clinical load, which implies that digital disruption can propagate systemically rather than remain institutionally contained. WHO's 2024 technical consultation similarly frames cybersecurity in digital health as a resilience problem rather than a narrow IT problem, emphasizing that infrastructure weakness, low-resource settings, and limited technical capacity intensify vulnerability.

A third strand of the reviewed literature addresses health IT safety hazards, information integrity problems, and technology-induced error. Kim et al. (2017) systematically review health IT problems and show that issues related to user interaction, interface design, access problems, configuration, and software changes can interfere with care delivery and, in many studies, are linked to patient harm and even death. Bowman (2013) adds that poor system design and improper use can compromise information integrity through data loss, incorrect entry, flawed display, and transmission errors, thereby creating direct safety and quality implications. Palojoki et al. (2016) similarly find that EHR users perceive extended system unavailability as a high-risk safety concern and argue that proactive and systematic assessment of HER related risk is necessary before harmful events occur. Borycki and Kushniruk (2023) reinforce this by showing that digital technologies can both improve safety and introduce new error pathways, meaning that digital health systems should be understood as sociotechnical safety environments rather than neutral tools.

A fourth cluster relates to AI-specific fragility and deployment risk. Cross et al. (2024) show that bias in medical AI can emerge across the full AI lifecycle from data and labels to development, evaluation, deployment, and end-user interaction and can produce substandard clinical decisions and reinforce health inequalities if not properly addressed. Norori et al. (2021) similarly argue that AI in health care inherits and amplifies data-driven, algorithmic, and human bias, especially where populations are underrepresented or misrepresented in biomedical datasets. The WHO paper on AI accountability and safety further emphasizes that AI-based clinical tools operate in a safety-critical domain in which failure can directly harm patients and where conventional accountability and assurance practices remain insufficiently adapted. These concerns are highly relevant to the present paper because one of the mechanisms discussed by your study is the mismatch between testing or training environments and real deployment contexts, a condition that may force systems out of the service pathway altogether when real-world performance becomes unreliable.

The literature also shows that telemedicine and digital access solutions are highly infrastructure-contingent. Fontalvo et al. (2025) identify a threshold effect in rural telehealth, showing that telehealth investment has limited effect below a minimum level of rural internet penetration and that infrastructure should be treated as a prerequisite rather than a complementary factor. Tilhou et al. (2023) show that telehealth expansion is associated with internet speed and that digital access disparities persist even when telehealth availability increases. Maita et al. (2024) further conclude that although digital tools can improve access in rural populations, limited connectivity and low familiarity with digital tools remain significant barriers. This strand of evidence is directly relevant to the problem of digitally dependent service models in remote settings: if a care model is designed around telemedicine without adequate infrastructure resilience or backup arrangements, disruption can translate immediately into service loss. Another study on AI for Health Equity reinforces this argument from a health-systems angle. It shows that AI may reduce urban–rural disparities only when digital infrastructure, interoperability, trust, and local capacity are sufficiently developed, and it explicitly treats digital health as a socio-technical ecosystem rather than a purely technological upgrade (Hojabri & Manafi, 2025; Hojabri & Manafi,2026a). The literature reviewed also provides a strong collapse-oriented systems framework for interpreting these digital risks. In the Early Warning Framework, digital and information system failure is identified as one of the seven core determinants of healthcare system collapse, alongside governance failure, financial fragility, workforce burnout, infrastructure vulnerability, erosion of trust, and loss of adaptability (Hojabri & Manafi, 2026a). The same study explicitly interprets digital system failure as a condition in which data are used for reporting and control rather than for learning and adaptation, linking digital problems to broader loss of system responsiveness and coordination. It also treats collapse as progressive and saturation-driven rather than sudden, thereby providing a conceptual bridge between digital disruption and larger systemic deterioration.

This collapse-oriented view is reinforced by the reviewed paper on health system models under pressure, which argues that resilience and collapse risk are better explained by imbalances among stability, efficiency, and adaptability than by institutional typology alone (Hojabri & Manafi, 2026 b). In practical terms, this means that digitally enhanced systems may appear high-performing according to conventional metrics while becoming more brittle under stress (Abed et al., 2024; Abbou et al., 2024; Kim et al., 2017; Bowman, 2013).

The Theory of Saturation and related conceptual papers deepen this interpretation. Manafi's (2025, 2026 a) orientation note defines saturation as a condition in which increasing inputs, speed, connectivity, and efficiency no longer improve performance but instead degrade stability, meaning, and adaptability. Klein and Manafi's (2026) article on digital saturation applies this logic directly to the age of AI, arguing that technological acceleration can outpace human, institutional, and structural adaptation, producing institutional inertia, technical fragility, burnout, and dysfunctional feedback loops. Even the more abstract uploaded papers on saturation and collapse in dynamical systems and PCA under saturation and collapse are relevant here, because they contribute a formal language of threshold effects, irreversibility, degeneration, and loss of stable structure once saturation exceeds adaptive capacity. Although these are not healthcare studies, they support the present paper's theoretical claim that collapse-prone behavior can emerge when highly optimized systems lose reversibility and degrade under accumulated structural load.

Across the uploaded literature, one additional theme is especially important: loss of redundancy and reversibility. Downtime studies repeatedly show that organizations cannot simply assume that paper-based or manual operations will work once digital systems fail; manual continuity requires training, rehearsal, user guides, backup viewers, emergency prescription systems, and organizational preparedness (Lyon et al., 2023; Jo et al., 2024). The practical meaning is clear: when repetitive recording, coordination, prescribing, and retrieval tasks are fully shifted to digital systems, the system may lose the ability to function coherently without them. In the present paper, this is one of the clearest signs of digital saturation.

Finally, the literature suggests that digital disruption may activate a secondary collapse mechanism through trust erosion. The Early Warning Framework (Hojabri & Manafi; 2026 a) treats erosion of trust and social capital as a distinct determinant of collapse and links it to weakened legitimacy and social cohesion. Repeated service interruptions, degraded information reliability, unstable AI outputs, failed telemedicine access, and visible dependence on brittle digital infrastructure all increase the risk that patients, staff, and institutions lose confidence in the system's reliability. Once this occurs, digital disruption no longer remains a technical or operational issue; it becomes a stability issue in SEA terms and may continue to affect the system even after the original technical failure has been resolved.

Taken together, the reviewed literature supports a strong synthesis: digital saturation in health systems is not merely the expansion of digital tools, but a multidimensional condition in which digital dependency, infrastructure fragility, cybersecurity exposure, AI deployment mismatch, loss of reversibility, performance-measurement blind spots, and trust erosion reinforce one another. Under such conditions, digital systems may function not only as performance enablers but also as risk amplifiers, especially where resilience aware design, backup capacity, contextual alignment, and adaptive support are weak. The gap in the literature is therefore not whether digital systems are useful they clearly are but how they should be designed, implemented, and supported so that their benefits do not turn into pathways toward temporary service collapse, chronic vulnerability, or broader systemic instability. Table 1 summarizes the main categories of challenges in digital health systems that may lead to service disruption, along with their key operational manifestations.

Table 1. Key Challenges in Digital Health Systems Leading to Service disruption

Main Category	Sub-Categories	Potential Impact on Service Delivery
Technical Failures	System downtime (EHR/HIS), software crashes, server failure	Immediate interruption of clinical workflows and documentation
Cybersecurity Threats	Ransomware, hacking, data breaches, unauthorized access	System shutdown, loss of data access, cancellation of services
Infrastructure Dependency	Internet failure, power outage, network instability, cloud disruption	Disruption of telemedicine and digital services, especially in remote areas
Workflow Over-Integration with IT	Full digitization of clinical processes, lack of modular workflows	Local failure leads to system-wide disruption (cascading effects)
Loss of Reversibility (No Manual Backup)	Elimination of paper-based systems, lack of manual skills, ineffective fallback processes	Inability to continue services during failure, slow recovery
AI and Algorithmic Failures	Bias, model degradation, mismatch between training and real-world data	Incorrect clinical decisions, system withdrawal from service
Data Integrity Issues	Incorrect data entry, data loss, transmission errors, system misconfiguration	Unsafe clinical decisions, reduced care quality
Interoperability Failures	Lack of system integration, data exchange failure between systems	Fragmented care, coordination breakdown
Lack of Preparedness and Support	Absence of training, weak downtime protocols, lack of backup systems	Severe disruption even during minor system failures
Trust and Behavioral Factors	Low user trust, resistance to digital systems, improper use	Reduced effectiveness of systems, increased errors

The reviewed literature reveals that disruptions in digital health systems arise from multiple sources, including system downtime, cybersecurity threats, infrastructure fragility, AI-related failures, and information integrity issues. As summarized in Table 2, these disruptions directly affect both healthcare service delivery and patient safety. In this table, findings indicate that digital system failures are not isolated technical events but systemic disruptions that can directly affect care continuity and patient safety. These patterns form the empirical basis for understanding digital saturation as a condition in which dependency, reduced adaptability, and system fragility converge. Table 2 shows Extracted Causes of Digital System Disruptions and Their Impact on Healthcare Delivery and Patient Safety.

Table 2 Extracted Causes of Digital System Disruptions and Their Impact on Healthcare Delivery and Patient Safety

Source (Study)	Type of Digital System	Identified Cause of Disruption	Key Challenge Described	Impact on Service Delivery	Impact on Patient Safety
Larsen et al. (2019)	HER	System downtime sys. viruses; upgrades; failure	Lack of continuity planning; poor documentation processes	Delays in laboratory reporting; disrupted workflows	Reduced accuracy of records; increased risk of clinical errors
Larsen et al. (2017)	HER	Downtime-related system failure	Weak adherence to downtime procedures; poor coordination	Disruption in medication ordering, lab processes, communication	Patient safety incidents (identification errors, medication risks)
Lyon et al. (2023)	EHR/HIS	Ineffective downtime management	Lack of training, drills, and preparedness	Inability to maintain service continuity during outages	Unsafe transition to manual processes
Jo et al. (2024)	HIS	Failure of backup systems	Manual fallback systems ineffective; lack of real-time alternatives	Service interruption during scheduled/unplanned downtime	Delayed or incorrect treatment decisions
Abbou et al. (2024)	Hospital-wide digital systems	Cyberattack (complete shutdown)	Full dependency on digital systems; lack of resilience mechanisms	Organization-wide disruption of clinical services	Risk to all patients due to loss of system functionality
Neprash et al. (2022)	Health IT infrastructure	Ransomware attacks	Increasing cyber threats; weak preparedness	Cancellation of services; ambulance diversion; delayed care	Indirect harm due to delayed or inaccessible care
Kim et al. (2017)	Health IT systems	IT-related errors and failures	Interface problems, access issues, configuration errors	Delayed care; workflow inefficiencies	Patient harm and even mortality linked to IT failures
Bowman (2013)	HER	Information integrity failure	Data entry errors; system misuse; poor design	Inaccurate or incomplete information flow	Clinical decision errors and safety risks
Palojoki et al. (2016)	HER	System unavailability	High reliance on digital systems in critical units	Disruption in ED, ICU, and OR workflows	High perceived and actual safety risk
Borycki & Kushniruk (2023)	Digital health systems	Technology-induced errors	Poor integration of technology into workflows	Error propagation across systems	Increased likelihood of adverse events
Cross et al. (2024)	AI systems	Bias and model failure	Bias across AI lifecycle; poor generalization	Reduced reliability of decision support	Unsafe or inequitable clinical decisions
Norori et al. (2021)	AI systems	Data bias and representation issues	Underrepresentation of populations	Misdiagnosis or inappropriate recommendations	Inequitable and unsafe outcomes
Fontalvo et al. (2025)	Telemedicine	Infrastructure threshold failure	Low internet penetration in rural areas	Failure of telehealth services	Reduced access to timely care
Tilhou et al. (2023)	Telehealth	Connectivity limitations	Digital inequality persists despite expansion	Unequal access to services	Delayed or missed care in underserved groups
Maita et al. (2024)	Digital health tools	Low digital literacy and infrastructure gaps	Limited user capability; weak adoption	Ineffective service delivery	Increased risk of improper care use

3. Methodology

This study adopts a qualitative research approach to examine how dependency on digital and information systems may introduce systemic vulnerabilities in healthcare and to identify resilience-oriented design and support considerations for complex care environments. The study is grounded in the perspective that disruptions in digital systems are not merely technical failures but may evolve into system-level risks affecting service continuity, recovery capacity, and public trust. Accordingly, the research focuses on generating theoretically informed insights into how such disruptions occur and how they can be mitigated through improved system design and support.

Data were collected through semi-structured interviews with participants selected using a purposive sampling strategy. The interview protocol was informed by prior literature on digital health disruptions and structured using the Stability–Efficiency–Adaptability (SEA) model to ensure systematic coverage of key system dimensions. As shown in Table 3, the interview framework was designed to explore issues related to digital dependency (efficiency), resilience and fallback capacity (adaptability), and service continuity and trust (stability).

Table 3. interview questions

SEA Dimension	Focus Area	Questions
Efficiency	Digital Dependency	To what extent are your core processes dependent on digital and information systems?
Efficiency	Automation & Workflows	Which processes are fully automated and cannot function without digital systems?
Efficiency	AI Integration	How are AI systems used in decision-making or operational processes?
Efficiency	Failure Sensitivity	Which digital systems cause immediate disruption when they fail?
Adaptability	Backup & Redundancy	What backup mechanisms exist when digital systems fail, and are they practically usable?
Adaptability	Reversibility	Can key processes be continued manually when digital systems are unavailable?
Adaptability	Infrastructure Resilience	How do systems function in low-connectivity or remote environments?
Adaptability	AI Deployment Gap	Have you observed differences between AI performance in testing and real-world conditions?
Adaptability	System Removal	Have digital or AI systems ever been removed due to poor performance? What were the reasons?
Stability	Service Continuity	What happens to service delivery when digital systems are disrupted?
Stability	Trust & Perception	How do patients and healthcare staff react to system failures?
Stability	Long-term Effects	Do repeated disruptions affect confidence in the healthcare system over time?
Stability	Social Impact	Can digital system failures lead to broader dissatisfaction or instability within the healthcare system?

A total of 13 participants were included in the study. The sample consisted of four stakeholder groups: health system managers and policymakers (n=3), healthcare providers including physicians and nurses (n=4), health information technology and digital system experts (n=3), and service users or patients (n=3). Participants were selected based on their direct or indirect experience with digital health systems, including exposure to system disruptions, operational dependency, or recovery processes. The sample size was considered sufficient to achieve thematic saturation, as recurring patterns and themes emerged consistently across interviews. Interviews were conducted using a semi-structured format and lasted between 30 and 60 minutes. All interviews were conducted online and audio-recorded with participants' consent. The recordings were transcribed for analysis.

The interviews explored key issues such as dependency on digital systems, vulnerability of automated workflows, availability and effectiveness of backup mechanisms, reversibility of processes, performance of AI systems under real-world conditions, continuity of services in infrastructure-constrained environments, and the impact of disruptions on trust and system stability.

Data were analyzed using thematic analysis, following an iterative process including initial coding, grouping of codes into broader themes, and abstraction into higher-level concepts. To enhance analytical depth, the SEA model was applied as an interpretive lens to map identified themes across system dimensions. In this context, digital dependency was primarily associated with efficiency-oriented optimization, while limitations in fallback mechanisms reflected reduced adaptability, and disruptions in service delivery were linked to challenges in system stability. To ensure analytical rigor, cross-case comparison and consistency checks were performed across interviews. Participation was voluntary, informed consent was obtained from all participants, and all data were anonymized to ensure confidentiality.

The methodological approach was designed not only to identify risks but also to derive actionable design and support considerations that can reduce the likelihood of service disruption, prevent temporary system collapse, and limit the progression toward broader systemic instability.

4. Results

The findings of this study reveal that disruptions in digital health systems are not isolated technical failures, but are rooted in structural imbalances across the three core dimensions of the Stability–Efficiency–Adaptability (SEA) model. Across the 13 interviews, participants consistently described healthcare systems as increasingly optimized for efficiency, while exhibiting reduced stability under disruption and limited adaptability in response to system failures. From a stability perspective, digital systems were reported to be highly sensitive to disruption. The majority of participants (11 out of 13) indicated that failures in core systems such as electronic health records (EHRs), hospital information systems, or network connectivity lead to immediate interruption of clinical workflows. Even short-term disruptions were described as having significant operational consequences (reported by 9 participants). These findings suggest that stability is strongly dependent on continuous system availability, with limited capacity to absorb shocks. As one participant noted, "When the system goes down, everything stops immediately." This reflects a condition in which system stability is contingent upon uninterrupted digital functionality. In relation to efficiency, participants widely acknowledged the benefits of digital transformation. Systems were described as highly effective in improving documentation, coordination, and workflow speed. However, these efficiency gains were associated with structural trade-offs. Most participants (12 out of 13) reported that core processes are fully digitized, and 9 participants indicated that no viable alternative workflows exist. This high level of process centralization reduces redundancy and increases dependency on system performance. As highlighted by one participant, “Everything is faster and more organized, but only when the system works.” This suggests that efficiency-driven design may contribute to system vulnerability by reducing flexibility and buffering capacity.

From an adaptability perspective, the findings indicate a limited ability to respond to and recover from disruptions. A majority of participants (11 out of 13) reported that manual fallback mechanisms are either ineffective or impractical, while 7 participants indicated that preparedness measures are largely theoretical rather than operational. Participants emphasized that staff are often not trained to operate without digital systems, and that manual processes are incomplete or inefficient. One participant explained, “We have backup plans, but in practice, they don’t work.” These findings demonstrate a reduced adaptive capacity, where systems struggle to adjust to unexpected conditions. Additional adaptability challenges were identified in relation to AI and advanced digital tools. Participants (9 out of 13) reported discrepancies between expected and real-world performance of AI systems, often due to contextual variability or data mismatch. In some cases, systems were partially or fully withdrawn from use (reported by 4 participants), reflecting limitations in real-world applicability and trust.

Across all dimensions, the findings also highlight cross-dimensional interactions. Disruptions were frequently described as cascading across interconnected systems, indicating that failures in one component can rapidly affect others. This reflects a combined effect of reduced stability (due to disruption sensitivity), efficiency-driven integration (which amplifies failure propagation), and limited adaptability (which slows recovery). Furthermore, repeated disruptions were associated with erosion of trust among both healthcare providers and patients (reported by 11 participants), suggesting that digital instability may extend beyond operational impacts to affect system legitimacy.

Overall, the findings in table 4 demonstrate a clear imbalance within the SEA model: high efficiency, reduced stability, and limited adaptability. This imbalance creates conditions in which healthcare systems perform effectively under normal circumstances but become increasingly fragile under stress. These results provide an empirical basis for understanding how digital systems may contribute to systemic vulnerability.

Table 4. Interview Findings Mapped to Disruption Factors within the SEA Model

Disruption Factor	SEA Dimension	Key Findings (n=13)	Illustrative Quotes	Impact on Service Delivery
Technical Failures	Stability	11 participants reported immediate disruption; 9 reported impact even for short downtime	"When the system goes down, everything stops."	Immediate workflow interruption
Cybersecurity Threats	Stability	8 participants identified high-impact disruption; 5 noted risk of full shutdown	"If systems are locked, we cannot continue anything."	Service shutdown and delays
Infrastructure Dependency	Stability	10 participants reported dependency on connectivity; 6 highlighted severe issues in remote settings	"Without stable internet, the system is unusable."	Disruption of remote care and access
Workflow Over-Integration	Efficiency	12 participants reported full digitalization; 9 reported no alternative workflows	"Everything depends on the system."	Full dependency and system-wide disruption
Loss of Reversibility	Adaptability	11 participants reported ineffective manual fallback; 7 reported lack of preparedness	"Manual processes are not realistic anymore."	Inability to continue services
AI and Algorithmic Failures	Adaptability	9 participants reported performance mismatch; 4 reported system withdrawal	"AI works differently in real conditions."	Reduced reliability of decision support
Data Integrity Issues	Stability	7 participants reported incomplete or delayed data during disruptions	"Data is sometimes missing or delayed."	Risk of incorrect decisions
Interoperability Failures	Stability / Efficiency	6 participants reported coordination issues between systems	"Systems don't communicate well."	Fragmented workflows
Lack of Preparedness	Adaptability	10 participants reported impractical backup systems	"Backup plans are not usable."	Increased disruption severity

Trust and Behavioral Factors	Stability	11 participants reported reduced trust due to repeated failures	“People lose trust when systems fail repeatedly.”	Reduced system confidence

5. Discussion

The findings of this study provide strong empirical support for understanding disruptions in digital health systems through the lens of the Stability–Efficiency–Adaptability (SEA) model. Rather than viewing digital system failures as isolated technical events, the results indicate that such disruptions emerge from structural imbalances across these three core dimensions. From a stability perspective, the findings reveal that healthcare systems have become increasingly sensitive to disruption due to their high level of dependency on digital infrastructures. Participants consistently reported that failures in core systems such as electronic health records, network connectivity, or integrated platforms lead to immediate interruption of clinical and administrative processes. This suggests that system stability is no longer maintained through redundancy or buffering mechanisms, but is instead contingent upon continuous digital functionality. As a result, even short-term disruptions can have disproportionate impacts on service delivery.

In contrast, the efficiency dimension appears to be highly developed. Digital transformation has significantly improved workflow speed, coordination, and data accessibility. However, the results indicate that these efficiency gains are achieved through extensive process centralization and automation, often accompanied by the reduction of redundancy and alternative pathways. This efficiency-driven design, while beneficial under normal operating conditions, contributes to structural rigidity. In SEA terms, the overemphasis on efficiency appears to come at the expense of both stability and adaptability, creating conditions in which systems are optimized for performance but not for resilience. The most critical limitation identified in the findings relates to adaptability. The study shows that healthcare systems have a limited capacity to respond to and recover from disruptions. Manual fallback processes are often impractical, staff are insufficiently trained to operate outside digital environments, and backup mechanisms are frequently theoretical rather than operational. These conditions indicate a loss of reversibility, where systems are unable to revert to alternative modes of operation when disruptions occur. Furthermore, challenges associated with AI systems such as performance gaps between testing and real-world environments highlight additional constraints on adaptive capacity.

Taken together, these findings point to a clear SEA imbalance, characterized by high efficiency, reduced stability, and limited adaptability. This imbalance creates a systemic condition in which healthcare systems perform effectively under stable conditions but become increasingly fragile under stress. In this context, the concept of digital saturation can be understood as the outcome of accumulated dependency, reduced flexibility, and heightened sensitivity to disruption. Importantly, the study also demonstrates that digital system disruptions are not confined to operational inefficiencies but extend to broader system-level consequences. The propagation of failures across interconnected systems, combined with prolonged recovery times and repeated disruptions, contributes to erosion of trust among both healthcare providers and patients. This suggests that instability in digital systems may undermine not only service delivery but also the perceived reliability and legitimacy of healthcare institutions.

Based on these findings, this study highlights the need to move beyond efficiency-driven approaches in digital health system design and to incorporate resilience-oriented principles that restore balance across the SEA dimensions. This includes strengthening system stability through redundancy and modularity, enhancing adaptability through functional fallback mechanisms and training, and ensuring that efficiency gains do not compromise system robustness. A key implication of this study is the potential to translate these insights into a practical assessment approach for healthcare organizations. The disruption factors identified through the literature and validated through interviews provide a foundation for developing a structured, checklist-based evaluation tool that enables organizations to assess their level of digital saturation. Given the multi-dimensional nature of the identified challenges, such an assessment should be conducted through a multi-stakeholder committee-based process, incorporating perspectives from clinical staff, information technology experts, and organizational leadership. The use of structured consensus methods, such as Delphi-informed approaches, may further enhance the reliability and validity of the assessment.

While the present study focuses on identifying and conceptualizing the mechanisms of digital disruption, future research can build on these findings by developing and validating such assessment tools. A checklist-based framework could enable healthcare organizations and health systems to periodically evaluate their digital dependency, resilience capacity, and vulnerability to disruption, thereby supporting proactive planning and targeted interventions. By quantifying areas of weakness and strength, such tools may contribute to the design of more resilient, adaptable, and sustainable digital health systems.

In conclusion, this study demonstrates that digital transformation in healthcare, while essential, may introduce new forms of systemic risk when not balanced across stability, efficiency, and adaptability. Addressing these imbalances is critical to ensuring that digital systems function not only as enablers of performance, but also as foundations for resilient and reliable healthcare delivery.

Declaration of AI Assistance: *We hereby declare that artificial intelligence tools (ChatGPT by OpenAI) were used solely for language editing and refinement of this article. The content, ideas, and analysis were developed by the author, while AI assistance was limited to improving clarity, grammar, and style.*

References

Abed, S. F., Allain-Ioosa, S., & Shindo, N. (2024). *Examining the threat of cyber-attacks on health care during the COVID-19 pandemic*. World Health Organization.

Abbou, B., Kessel, B., Ben Natan, M., Gabbay-Benziv, R., Dahan Shriki, D., Ophir, A., Goldschmid, N., Klein, A., Roguin, A., & Dudkiewicz, M. (2024). When all computers shut down: The clinical impact of a major cyber-attack on a general hospital. *Frontiers in Digital Health, 6*, 1321485.

Bowman, S. (2013). Impact of electronic health record systems on information integrity: Quality and safety implications. *Perspectives in Health Information Management, 10*(Fall).

Borycki, E. M., & Kushniruk, A. W. (2023). Health technology, quality and safety in a learning health system. *Healthcare Management Forum, 36*(2), 79–85.

Cross, J. L., Choma, M. A., & Onofrey, J. A. (2024). Bias in medical AI: Implications for clinical decision-making. *PLOS Digital Health, 3*(11), e0000651.

Fontalvo, H. R., Rico, F., de la Puente, M., Torres, J., & Guzman, H. (2025). When telehealth fails rural communities: The 40% internet threshold that changes everything. *Digital Health, 11*, 1–16.

Gates, L. G. (2024). Cyber attacks on interoperable electronic health records: A clear and present danger. *Missouri Medicine, 121*(1), 6–9.

Gutowski, P., Hojabri, R., & Manafi, M. (2026). Performance measurement in health systems: A SEA model reinterpretation of system capacity, saturation, and collapse. *Journal of Saturation Studies*.

Hojabri, R., & Manafi, M. (2025). AI for Health Equity: Bridging the Urban–Rural. *Journal of Creative Perspectives*, *1*(4), 65-71.

Hojabri, R., & Manafi, M. (2026a). An Early Warning Framework for Healthcare System Collapse. *Journal of Saturation Studies*, *1*(1), 20-34.

Hojabri, R., & Manafi, M. (2026b). Health system models under pressure: A comparative assessment of saturation and collapse risks through the SEA framework. *Journal of Saturation Studies, Special Issue*.

Hojabri, R., Borousan, E., & Manafi, M. (2012). Impact of using telemedicine on knowledge management in healthcare organizations: A case study. *African Journal of Business Management*, *6*(4), 1604.

Jo, I., Kim, W., Lim, Y., Kang, E., Kim, J., Chung, H., & Kim, J. (2024). Strategy for scheduled downtime of hospital information systems utilizing third-party applications. *BMC Medical Informatics and Decision Making, 24*, 300.

Kim, M. O., Coiera, E., & Magrabi, F. (2017). Problems with health information technology and their effects on care delivery and patient outcomes: A systematic review. *Journal of the American Medical Informatics Association, 24*(2), 246–260.

Larsen, E., Fong, A., Wernz, C., & Ratwani, R. M. (2017). Implications of electronic health record downtime: An analysis of patient safety event reports. *Journal of the American Medical Informatics Association*.

Larsen, E., Hoffman, D., Rivera, C., Kleiner, B. M., Wernz, C., & Ratwani, R. M. (2019). Continuing patient care during electronic health record downtime. *Applied Clinical Informatics, 10*(3), 495–504.

Lyon, R., Jones, A., Burke, R., & Baysari, M. T. (2023). What goes up must come down: A state-of-the-art electronic health record downtime and uptime procedure. *Applied Clinical Informatics, 14*(3), 513–520.

Maita, K. C., Maniaci, M. J., Haider, C. R., Avila, F. R., Torres-Guzman, R. A., Borna, S., Lunde, J. J., Coffey, J. D., Demaerschalk, B. M., & Forte, A. J. (2024). The impact of digital health solutions on bridging healthcare access in rural areas: A scoping review. *The Permanente Journal, 28*, 23–134.

Manafi, M. (2025). Orientation note: Saturation, collapse, and the Rosetta Stone model. Manafi Institute for Saturation Studies. https://manafi-institute.de/Resources

Manafi, M. (2026). The Theory of Saturation, Collapse Model, and Rosetta Stone Model: A Unified yet Modular Meta-Framework. Journal of Saturation Studies, 1(1), 10-19.

Manafi, M., & Klein, M. (2026). Digital Saturation: Institutional Inertia and Cultural Transformation in the Age of AI. *Journal of Saturation Studies*, *1*(1), 43-54.

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021. *JAMA Health Forum, 3*(12), e224873.

Norori, N., Hu, Q., Aellen, F. M., Faraci, F. D., & Tzovara, A. (2021). Addressing bias in big data and AI for health care: A call for open science. *Patterns, 2*(10), 100347.

Palojoki, S., Pajunen, T., Saranto, K., & Lehtonen, L. (2016). Electronic health record-related safety concerns: A cross-sectional survey of electronic health record users. *JMIR Medical Informatics, 4*(2), e13.

Tilhou, A. S., Jain, A., & DeLeire, T. (2023). Telehealth expansion, internet speed, and primary care access before and during COVID-19. *JAMA Network Open*.

World Health Organization. (2020). Artificial intelligence in health care: Accountability and safety.

World Health Organization. (2024). *Addressing future cybersecurity threats in digital health: Report of the technical consultation, Geneva, Switzerland, 12–14 December 2023*.

World Health Organization. (2024). *Examining the threat of cyber-attacks on health care during the COVID-19 pandemic*.

Acknowledgement
This research was supported by the Manafi Institute for Saturation Studies (MISS).