Digital Saturation Assessment in healthcare systems based on SEA Model

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

The increasing integration of digital and information systems in healthcare has significantly improved efficiency, coordination, and access to services. However, growing dependency on these systems may also introduce systemic vulnerabilities, leading to conditions conceptualized as digital saturation. While prior research has identified the mechanisms through which digital systems contribute to disruption, there remains a lack of practical tools for assessing this phenomenon at the organizational level.

This study aims to develop and validate a structured checklist-based instrument for assessing digital saturation in healthcare organizations, grounded in the Stability–Efficiency–Adaptability (SEA) model. The study adopts a multi-phase design, beginning with the generation of checklist items derived from previously identified disruption factors, including digital dependency, workflow integration, reversibility, infrastructure reliability, cybersecurity, and AI-related limitations. These items are subsequently refined through a Delphi-based consensus process involving experts from clinical, technical, and managerial domains.

The resulting checklist is designed to enable systematic and periodic evaluation of digital system vulnerability across healthcare settings. In addition, a scoring framework is proposed to support the quantification of digital saturation levels and facilitate comparison across organizational units. By translating conceptual insights into an operational assessment tool, this study contributes to bridging the gap between digital health research and practice, providing healthcare organizations with a practical mechanism for identifying vulnerabilities, prioritizing interventions, and enhancing system resilience.

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

1. Introduction

Health systems are increasingly being reshaped by digital transformation, driven by the rapid expansion of electronic health records (EHRs), digital imaging and laboratory systems, artificial intelligence (AI), and telemedicine infrastructures. These technologies are widely promoted as mechanisms for improving clinical quality, enhancing cost-efficiency, strengthening care coordination, and expanding access to services (Abed et al., 2024; Larsen et al., 2019). This promise is particularly critical in rural and geographically remote settings, where telehealth and digital care models are often positioned as key solutions to overcome persistent barriers related to distance, workforce shortages, and limited-service availability (Hojabri et al., 2012; Fontalvo et al., 2025; Hojabri & Manafi, 2025).

However, alongside these benefits, the literature increasingly highlights a parallel structural shift: the emergence of systemic digital dependence. As emphasized in the WHO report on cyberattacks in healthcare, the transition toward digital systems not only enhances efficiency and safety but also introduces new vulnerabilities, as healthcare delivery becomes reliant on infrastructures that can be targeted by ransomware and other cyber threats (WHO, 2024; Abed et al., 2024). Evidence from EHR downtime studies reinforces this concern, showing that when core digital systems become unavailable, essential care processes are disrupted, clinical decision support mechanisms are deactivated, and patient safety may be compromised (Larsen et al., 2019). Similarly, empirical analyses of hospital cyberattack demonstrate that in highly integrated digital environments, disruptions rarely remain localized; instead, they propagate across clinical, administrative, logistical, and communication systems, often requiring prolonged recovery periods (Abbou et al., 2024).

These risks become more pronounced when examined through the lens of digital saturation. Klein and Manafi (2026) conceptualize saturation as a condition in which the pace of technological advancement exceeds the adaptive capacity of human, organizational, and institutional structures, resulting in rigidity, recursive dysfunction, and eventual breakdown rather than sustained improvement. This perspective aligns with Manafi's (2025) broader theory of saturation, which frames crises and collapse not as isolated events but as the cumulative outcome of overload, compressed feedback loops, and declining adaptive capacity. Within health systems research, similar dynamics are observed in studies showing that continuous pressure toward optimization and efficiency can erode system buffers, reduce flexibility, and gradually push systems toward saturation and functional fragility (Hojabri & Manafi, 2026a, 2026b).

Importantly, these vulnerabilities are not limited to large-scale disruptions such as outages or cyberattacks. Research on health information technology demonstrates that IT-related problems can interfere with care delivery, generate information errors, and in some cases lead to patient harm, while existing reporting systems often fail to capture these impacts in a structured and systematic way (Kim et al., 2017). AI introduces an additional layer of risk: performance in controlled testing environments does not necessarily translate into safe or equitable real-world outcomes, particularly when deployment contexts differ from training data, leading to risks such as misclassification, false alerts, missed diagnoses, and biased clinical decision-making (Cross et al., 2024). Telemedicine systems are similarly contingent on infrastructure conditions; evidence suggests that in settings with weak digital infrastructure, investments in telehealth may yield limited benefits, with meaningful improvements emerging only after minimum connectivity thresholds are achieved (Fontalvo et al., 2025).

From a systems perspective, these disruptions are significant because healthcare system collapse is increasingly understood as a progressive, saturation-driven process rather than a single catastrophic event (Hojabri & Manafi, 2026b). The SEA model provides a useful analytical framework in this context by interpreting collapse as the result of sustained imbalance among stability, efficiency, and adaptability. In particular, an excessive focus on efficiency may weaken adaptive capacity and increase systemic fragility over time (Hojabri & Manafi, 2026b). Complementing this perspective, the Early Warning Framework developed by Hojabri and Manafi (2026a) identifies digital and information system failure as one of the seven core determinants of healthcare system collapse, linking it to the use of data primarily for reporting and control rather than for learning and adaptation.

Against this background, the present study aims to assess how digital dependency evolves into a pathway for service disruption and broader systemic vulnerability in healthcare systems. Beyond a conceptual contribution, this study develops and introduces a structured measurement tool designed to quantify the level of digital saturation in healthcare systems. Grounded in the SEA model, the proposed framework operationalizes digital saturation across three core dimensions stability, efficiency, and adaptability allowing each dimension to be assessed independently while also contributing to an integrated composite index of digital saturation in healthcare.

By conceptualizing digital transformation through the lens of digital saturation and embedding this within a measurable SEA-based structure, the study shifts the analytical focus from digital adoption alone toward the conditions required for resilient system performance. It argues that digital technologies should be understood not only as enablers of performance but also as critical infrastructures that may amplify systemic risk when redundancy, fallback capacity, infrastructure resilience, contextual alignment, and long-term support mechanisms are insufficiently developed. In doing so, the study contributes to the Information Systems literature by providing both a conceptual and operational framework for identifying early warning signals of digital overload, thereby supporting the prevention of temporary service disruptions, erosion of trust, and longer-term systemic instability.

2. Literature Review

Digital transformation has emerged as a defining structural feature of contemporary health systems, driven by the widespread adoption of electronic health records (EHRs), hospital information systems (HIS), telemedicine, artificial intelligence (AI), and digitally mediated care infrastructures. The literature consistently highlights the role of these technologies in enhancing efficiency, improving coordination of care, strengthening clinical decision-making, and expanding access to services ,particularly in geographically remote and underserved settings (Hojabri & Manafi, 2026a; Larsen et al., 2019; Maita et al., 2024; Tilhou et al., 2023).

However, beyond these benefits, the reviewed evidence points to a deeper structural transformation: the emergence of systemic dependence on digital infrastructures for routine service continuity. As emphasized in the WHO report on cyber threats, the transition from paper-based to digital systems simultaneously enhances performance and creates new forms of vulnerability, as healthcare delivery becomes increasingly exposed to cyber risks and technological failures (WHO, 2024; Abed et al., 2024). This dependency is further evidenced in hospital-level studies showing that EHR downtime immediately disrupts care coordination, laboratory reporting, clinical documentation, and patient safety processes (Larsen et al., 2017; Larsen et al., 2019).

A substantial body of literature focuses on operational fragility associated with EHR and HIS downtime. Larsen et al. (2019) demonstrate that system downtime significantly delays laboratory reporting and complicates data capture at critical moments of care delivery. Their earlier work (Larsen et al., 2017) identifies key patient safety risks during downtime, particularly in medication management, patient identification, and clinical communication. Importantly, studies by Lyon et al. (2023) and Jo et al. (2024) show that resilience during such disruptions cannot be assumed; rather, it must be actively designed through backup systems, user training, simulation exercises, emergency protocols, and organizational coordination. This highlights that digital resilience is not merely technological but organizational and behavioral in nature.

Cybersecurity threats represent a second major dimension of digital fragility. Empirical evidence shows that large-scale cyberattacks can shut down entire hospital systems, disrupting clinical operations and compromising care continuity (Abbou et al., 2024). Neprash et al. (2022) further document the rapid increase in ransomware attacks in healthcare, many of which result in service cancellations, ambulance diversion, and prolonged downtime. Notably, these disruptions are not confined to individual institutions; they may propagate across networks, redistributing patient load and creating systemic stress. The WHO (2024) framework accordingly reframes cybersecurity as a core resilience issue, particularly in low-resource settings where infrastructure limitations and technical capacity gaps exacerbate vulnerability.

A third line of research addresses safety risks and technology-induced errors in digital health systems. Kim et al. (2017) show that usability issues, interface design flaws, configuration errors, and system updates can interfere with care delivery and, in some cases, lead to patient harm. Similarly, Bowman (2013) highlights risks to information integrity arising from data entry errors, flawed system design, and transmission failures. Palojoki et al. (2016) emphasize that prolonged system unavailability is perceived by clinicians as a high-risk safety condition, underscoring the need for proactive risk assessment. Borycki and Kushniruk (2023) conceptualize digital health environments as sociotechnical systems in which technology both enhances safety and introduces new pathways for error, reinforcing the need for integrated safety frameworks.

AI deployment introduces an additional layer of complexity and risk. Cross et al. (2024) demonstrate that bias can emerge throughout the AI lifecycle—from data collection and model development to deployment and user interaction—potentially leading to suboptimal clinical decisions and reinforcing health inequities. Norori et al. (2021) similarly argue that AI systems inherit and amplify existing biases, particularly when datasets are incomplete or unrepresentative. WHO guidance on AI safety further stresses that healthcare AI operates in a safety-critical domain where failures can directly harm patients, while accountability mechanisms remain underdeveloped. A key issue identified in this literature is the mismatch between controlled development environments and real-world deployment contexts, which may lead to system unreliability and eventual exclusion from care pathways.

The effectiveness of telemedicine and digital access solutions is also shown to be highly dependent on underlying infrastructure. Fontalvo et al. (2025) identify a threshold effect, demonstrating that telehealth investments yield limited benefits below a minimum level of internet penetration. Tilhou et al. (2023) confirm that digital access disparities persist despite increased availability of telehealth services, while Maita et al. (2024) highlight connectivity limitations and digital literacy as key barriers. These findings suggest that digital health models are inherently fragile when implemented without sufficient infrastructural support, particularly in rural or resource-constrained settings.

From a systems perspective, the reviewed literature aligns with collapse-oriented frameworks that interpret digital risks as part of broader systemic vulnerability. The Early Warning Framework identifies digital system failure as one of the core determinants of healthcare system collapse, alongside governance failure, financial instability, workforce burnout, infrastructure fragility, erosion of trust, and loss of adaptability (Hojabri & Manafi, 2026a). Within this framework, digital failure is not merely technical but reflects deeper issues such as the use of data for control rather than learning, leading to reduced system responsiveness and coordination.

This perspective is reinforced by the SEA (Stability, Efficiency, Adaptability) model, which suggests that system performance and collapse risk are better understood through imbalances among these three dimensions rather than through institutional typologies alone (Hojabri & Manafi, 2026b). In this context, digitally advanced systems may appear efficient yet become increasingly brittle under stress, revealing hidden vulnerabilities (Abed et al., 2024; Abbou et al., 2024; Kim et al., 2017; Bowman, 2013).

The Theory of Saturation further deepens this interpretation by conceptualizing a state in which increasing digitalization no longer improves performance but instead degrades stability and adaptability (Manafi, 2025; 2026a). Klein and Manafi (2026) extend this concept to the digital age, arguing that rapid technological acceleration can exceed the adaptive capacity of institutions, leading to burnout, technical fragility, and dysfunctional feedback loops. Supporting evidence from systems theory literature highlights the role of threshold effects, irreversibility, and structural degradation when systems exceed their adaptive limits.

A critical and recurring theme across the literature is the loss of redundancy and reversibility. Studies on system downtime consistently show that organizations cannot rely on ad hoc manual processes when digital systems fail; effective continuity requires pre-designed fallback mechanisms, training, and organizational preparedness (Lyon et al., 2023; Jo et al., 2024). This indicates that as systems become fully digitized, their ability to function without digital support diminishes—a key indicator of digital saturation.

Finally, the literature suggests that digital disruption can trigger a secondary collapse mechanism through erosion of trust. Repeated system failures, unreliable data, unstable AI outputs, and disrupted access to care undermine confidence among patients, providers, and institutions. According to the Early Warning Framework, such erosion of trust represents a critical pathway toward systemic instability, extending the impact of digital failures beyond operational disruption into the domain of structural collapse.

In synthesis, the reviewed literature demonstrates that digital saturation in health systems is a multidimensional phenomenon characterized by increasing digital dependency, infrastructure fragility, cybersecurity exposure, AI-related risks, loss of reversibility, and erosion of trust. Under these conditions, digital technologies act not only as performance enhancers but also as potential amplifiers of systemic risk. The key gap in the literature, therefore, is not whether digital systems are beneficial, but how they can be designed and governed to prevent their transformation into drivers of instability and collapse. Following Table1 shows extracted key challenges in digital health systems leading to services disruption in health systems.

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

3. Methodology

This study adopts a multi-phase methodological approach to develop and validate a structured checklist-based instrument for assessing digital saturation in healthcare systems. The design builds upon prior empirical findings that identified key disruption factors associated with digital system failures and their impact on healthcare service delivery. By integrating evidence from previous qualitative research with expert consensus methods, this study aims to translate conceptual insights into an operational assessment framework.

The initial phase of the study focused on item generation. Checklist items were derived from previous study identified disruption factors, including technical failures, cybersecurity threats, infrastructure dependency, workflow over-integration, loss of reversibility, AI-related limitations, data integrity issues, interoperability failures, lack of preparedness, and trust-related challenges. For each factor, multiple items were formulated to capture its operational manifestations within healthcare settings. The items were designed to be clear, context-relevant, and applicable across different organizational levels. In addition, each item was mapped to one of the three dimensions of the Stability–Efficiency–Adaptability (SEA) model to ensure that the checklist reflects the balance across core system properties.

To refine and validate the checklist, a Delphi methodology was employed. Experts were selected through purposive sampling to ensure representation across key stakeholder groups, including clinical professionals, health information technology specialists, and healthcare managers. A panel of 15 participants was targeted to capture diverse perspectives while maintaining feasibility of the consensus process.

The Delphi procedure was conducted in iterative rounds. In the first round, participants evaluated each item in terms of relevance and clarity and were invited to suggest modifications or additional items. Based on this feedback, the checklist was revised and redistributed in the second round, where participants reassessed the items to achieve convergence of opinions. Consensus thresholds were applied to determine which items should be retained, modified, or removed. A third round was conducted to finalize agreement.

Following the Delphi process, a refined checklist was constructed, consisting of validated items organized into domains corresponding to the identified disruption factors. Each item represents a specific aspect of digital system performance or vulnerability and is intended to be assessed at the organizational level.

To enable quantitative evaluation, a scoring framework was developed in which each item is rated using a Likert-type scale (e.g., 1 to 5), reflecting the extent to which the condition is present within the organization. Scores across items are aggregated to produce a composite measure of system vulnerability. Based on this approach, a Digital Saturation Index (DSI) is defined as a normalized composite score, providing a quantitative representation of the system's level of digital saturation.

To support interpretation, the DSI is categorized into predefined ranges corresponding to different levels of system vulnerability, enabling organizations to identify whether they are in a safe, moderate, high-risk, or saturated state. In addition to the overall index, domain-level scores allow for the identification of specific areas of weakness across the SEA dimensions.

Participation in the Delphi process was voluntary, and informed consent was obtained from all participants. All responses were anonymized to ensure confidentiality and to minimize potential bias in expert evaluations.

Digital Saturation Index (DSI) Calculation

To enable quantitative assessment, a structured scoring approach was applied to the checklist items. Each item was rated using a five-point scale reflecting the extent to which the described condition is present within the system (1 = not present, 5 = very high).

All items were formulated in a risk-oriented manner, such that higher scores consistently indicate higher levels of digital vulnerability and saturation.

The total score was calculated as the sum of all item scores. Given a minimum possible score of 44 and a maximum of 220, the Digital Saturation Index (DSI) was defined as a normalized composite measure:

$$DSI = \frac{Total\ Score - 44}{176} \times 100$$

This transformation scales the index to a range of 0 to 100, where higher values indicate greater levels of digital saturation and system vulnerability.

The DSI enables comparison across organizations and supports identification of relative risk levels associated with digital system dependency and imbalance across the Stability–Efficiency–Adaptability (SEA) dimensions.

4. Results

The results of this study reflect the systematic development and refinement of a structured checklist for assessing digital saturation in healthcare systems, along with the operationalization of a composite Digital Saturation Index (DSI). The initial set of checklist items was derived from disruption factors identified in prior empirical research, which highlighted key mechanisms through which digital systems may contribute to service disruption and system vulnerability. These factors included technical failures, cybersecurity threats, infrastructure dependency, workflow over-integration, loss of reversibility, AI-related limitations, data integrity issues, interoperability challenges, lack of preparedness, and trust-related factors. Based on these domains, an initial pool of 44 items was generated to capture different dimensions of digital system performance and vulnerability. All items were formulated in a risk-oriented and consistent manner to ensure that higher scores directly indicate higher levels of digital saturation. This design decision eliminated the need for reverse scoring and minimized ambiguity during assessment, particularly in committee-based evaluation settings involving multiple stakeholders.

A Delphi-based consensus process was conducted to refine and validate the checklist. The expert panel consisted of representatives from clinical, technical, and managerial domains, ensuring a multi-dimensional perspective on digital system performance. In the first round, participants evaluated each item in terms of relevance and clarity. Feedback indicated that the items were largely comprehensive and aligned with real-world operational challenges. Minor revisions were made to simplify wording and improve interpretability across different user groups.

In the second round, the revised items were re-evaluated to assess agreement and consistency. A high level of convergence was observed among participants, and all items were retained with only minor refinements. No additional items were proposed, suggesting that the initial structure adequately captured the construct of digital saturation. The results of the Delphi process confirmed both the relevance and completeness of the identified domains.

The final checklist consists of 44 items organized into 11 domains, each representing a specific category of digital system vulnerability. These domains include digital dependency, workflow integration, reversibility, technical stability, cybersecurity, infrastructure reliability, AI performance, data integrity, interoperability, organizational preparedness, and trust-related factors. Each domain reflects a distinct aspect of how digital systems may contribute to operational fragility and service disruption. To enable quantitative assessment, a structured scoring approach was applied. Each item is rated on a five-point scale, where higher values indicate greater presence of risk conditions. The total score is calculated as the sum of all item scores, with a minimum possible score of 44 and a maximum of 220. To facilitate comparability and interpretation, the total score was normalized into a Digital Saturation Index (DSI) ranging from 0 to 100.

This transformation allows the index to represent the relative level of digital saturation across organizations or units. Higher DSI values indicate greater levels of system vulnerability, reflecting increased dependency on digital systems, reduced adaptability, and higher sensitivity to disruption. An interpretation framework was defined to support practical use of the index. Systems with lower DSI values are considered more stable and resilient, while higher values indicate increasing levels of risk and potential saturation. This classification enables healthcare organizations to identify their position and prioritize targeted interventions.

Importantly, the checklist and the DSI collectively provide a structured mechanism for assessing the balance across the Stability–Efficiency–Adaptability (SEA) dimensions. While efficiency-related aspects are reflected in workflow integration and process optimization, stability-related vulnerabilities are captured through system reliability, infrastructure dependency, and data integrity, and adaptability is represented through reversibility and preparedness. The results indicate that the developed instrument effectively captures imbalances across these dimensions, providing an operational representation of digital saturation.

The finalized checklist was structured using clear and uniformly worded, risk-oriented statements to ensure consistency in scoring. All items were designed such that higher scores directly reflect greater levels of digital vulnerability and saturation, minimizing ambiguity and eliminating the need for reverse scoring during committee-based assessment. Table 2 shows scoring meanings and Table no 3 checklists for assessing digital saturation in healthcare systems.

Table 2 , Threshold of score

Score	Meaning
1	Not at all
2	Low
3	Moderate
4	High
5	Very high

Table 3, Digital Saturation Checklists

No.	Domain	SEA Dimension	Statement (Risk Condition)	1 Not at all	2 Low	3 Moderate	4 High	5 Very High
1	Digital Dependency	Stability	High dependence of clinical processes on digital systems	☐	☐	☐	☐	☐
2	Digital Dependency	Stability	Inability to continue services without digital systems	☐	☐	☐	☐	☐
3	Digital Dependency	Stability	Critical decisions depend on digital data	☐	☐	☐	☐	☐

4	Digital Dependency	Stability	Lack of non-digital alternative workflows	☐	☐	☐	☐	☐
5	Workflow Integration	Efficiency	Full integration of workflows into digital systems	☐	☐	☐	☐	☐
6	Workflow Integration	Efficiency	Communication is fully dependent on digital systems	☐	☐	☐	☐	☐
7	Workflow Integration	Efficiency	Processes are primarily designed for efficiency and speed	☐	☐	☐	☐	☐
8	Workflow Integration	Efficiency	Redundant workflows have been eliminated	☐	☐	☐	☐	☐
9	Reversibility	Adaptability	Inability to perform tasks manually	☐	☐	☐	☐	☐
10	Reversibility	Adaptability	Staff cannot operate without digital systems	☐	☐	☐	☐	☐
11	Reversibility	Adaptability	Backup processes are not usable in practice	☐	☐	☐	☐	☐
12	Reversibility	Adaptability	Inability to recover quickly after disruptions	☐	☐	☐	☐	☐
13	Technical Stability	Stability	Frequent system downtime	☐	☐	☐	☐	☐
14	Technical Stability	Stability	High sensitivity to minor failures	☐	☐	☐	☐	☐
15	Technical Stability	Stability	Small failures lead to major disruptions	☐	☐	☐	☐	☐
16	Technical Stability	Stability	Low reliability of systems	☐	☐	☐	☐	☐
17	Cybersecurity	Stability	High vulnerability to cyberattacks	☐	☐	☐	☐	☐
18	Cybersecurity	Stability	Insufficient security measures	☐	☐	☐	☐	☐
19	Cybersecurity	Stability	Risk of access disruption due to cyber incidents	☐	☐	☐	☐	☐
20	Cybersecurity	Stability	Weak incident response capability	☐	☐	☐	☐	☐
21	Infrastructure	Stability	High dependence on internet connectivity	☐	☐	☐	☐	☐
22	Infrastructure	Stability	Service disruption due to power/network instability	☐	☐	☐	☐	☐
23	Infrastructure	Stability	Higher disruption in low-resource settings	☐	☐	☐	☐	☐
24	Infrastructure	Stability	Limited technical support availability	☐	☐	☐	☐	☐
25	AI Reliability	Adaptability	AI performs inconsistently in real settings	☐	☐	☐	☐	☐
26	AI Reliability	Adaptability	Low trust in AI outputs	☐	☐	☐	☐	☐
27	AI Reliability	Adaptability	Frequent need for human correction	☐	☐	☐	☐	☐
28	AI Reliability	Adaptability	AI systems abandoned due to poor performance	☐	☐	☐	☐	☐
29	Data Integrity	Stability	Incomplete or delayed data	☐	☐	☐	☐	☐
30	Data Integrity	Stability	Poor data quality affects decisions	☐	☐	☐	☐	☐
31	Data Integrity	Stability	System errors affect data reliability	☐	☐	☐	☐	☐
32	Data Integrity	Stability	Weak data quality control	☐	☐	☐	☐	☐
33	Interoperability	Efficiency	Lack of integration between systems	☐	☐	☐	☐	☐
34	Interoperability	Efficiency	Difficult data exchange between systems	☐	☐	☐	☐	☐

35	Interoperability	Efficiency	Delays or duplication due to incompatibility	☐	☐	☐	☐	☐
36	Interoperability	Efficiency	Poor coordination across departments	☐	☐	☐	☐	☐
37	Preparedness	Adaptability	Ineffective disruption management plans	☐	☐	☐	☐	☐
38	Preparedness	Adaptability	Staff not prepared for system failures	☐	☐	☐	☐	☐
39	Preparedness	Adaptability	Backup systems not regularly tested	☐	☐	☐	☐	☐
40	Preparedness	Adaptability	Insufficient emergency training	☐	☐	☐	☐	☐
41	Trust	Stability	Reduced staff confidence in systems	☐	☐	☐	☐	☐
42	Trust	Stability	Reduced patient trust due to disruptions	☐	☐	☐	☐	☐
43	Trust	Stability	Repeated disruptions causing dissatisfaction	☐	☐	☐	☐	☐
44	Trust	Stability	Users bypass digital systems	☐	☐	☐	☐	☐

To enable quantitative analysis of digital saturation, all checklist items were scored using a five-point scale, where higher values indicate greater presence of risk conditions associated with digital system vulnerability. The total score was calculated as the sum of all item responses. To provide a more granular understanding of system performance, the checklist items were grouped according to the Stability–Efficiency–Adaptability (SEA) model. Specifically, items were categorized into three dimensions: Stability (S), Efficiency (E), and Adaptability (A), reflecting different aspects of system behavior and vulnerability. For each dimension, a sub-score was calculated by summing the corresponding item scores. Given that the number of items differs across dimensions, all sub-scores were normalized to a scale of 0 to 100 to ensure comparability. The normalized sub-indices were calculated as follows:

$$SI = \frac{S_{raw} - S_{min}}{S_{max} - S_{min}} \times 100$$

$$EI = \frac{E_{raw} - E_{min}}{E_{max} - E_{min}} \times 100$$

$$AI = \frac{A_{raw} - A_{min}}{A_{max} - A_{min}} \times 100$$

where S_{raw}, E_{raw}, and A_{raw}represent the summed scores for Stability, Efficiency, and Adaptability items, respectively, and the minimum and maximum values correspond to the theoretical score ranges for each dimension. The overall Digital Saturation Index (DSI) was then calculated as the mean of the three normalized sub-indices:

$$DSI = \frac{SI + EI + AI}{3}$$

This approach ensures that each SEA dimension contributes equally to the overall index, regardless of the number of items assigned to each domain. Higher DSI values indicate greater levels of digital saturation, reflecting increased dependency on digital systems, reduced system flexibility, and heightened vulnerability to disruption. In addition to the overall index, the SEA-based sub-indices enable identification of specific sources of imbalance, allowing organizations to determine whether digital saturation is primarily driven by instability, excessive efficiency orientation, or lack of adaptability.

5. Conclusion

This study developed and operationalized a structured approach for assessing digital saturation in healthcare systems through the design of a checklist-based instrument and the introduction of the Digital Saturation Index (DSI). Building on empirically identified disruption factors, the study translated qualitative insights into a measurable framework that captures system-level vulnerability associated with increasing dependence on digital technologies.

A key contribution of this research lies in aligning the measurement of digital saturation with the Stability–Efficiency–Adaptability (SEA) model. By mapping checklist domains to SEA dimensions and deriving sub-indices, the study provides a theoretically grounded and operationally meaningful way to assess imbalance within healthcare systems. The findings suggest that digital saturation is not merely a function of technological expansion, but rather the result of disproportionate emphasis on efficiency without corresponding levels of stability and adaptability.

Importantly, the decision to structure the DSI based on SEA dimensions enhances its practical relevance for policymakers and healthcare managers. In contrast to generic digital maturity or performance assessments, the proposed index enables identification of specific sources of vulnerability, allowing decision-makers to distinguish whether risks arise from system fragility, over-integration, or insufficient adaptability. This provides a more actionable basis for designing targeted interventions aimed at strengthening system resilience.

The checklist and DSI together offer a scalable and interpretable tool that can be applied across healthcare organizations and systems to support monitoring, comparison, and strategic planning. By converting complex system dynamics into a structured and measurable format, the study bridges the gap between conceptual understanding and operational decision-making in digital health.

While the current study adopts an equal-weighting approach for simplicity and interpretability, future research may further refine the index by exploring alternative weighting schemes and validating the tool across different healthcare contexts. In addition, empirical application of the DSI in real-world settings will be essential to assess its predictive value and practical utility.

In conclusion, this study advances the understanding of digital transformation in healthcare by introducing digital saturation as a measurable construct and providing a SEA-based framework for its assessment. The proposed approach offers both theoretical and practical value, supporting more balanced and resilient digital health system development.

Discussion

The present study contributes to the growing body of research on digital transformation in healthcare by introducing digital saturation as a measurable and operational construct. While digital technologies have significantly enhanced efficiency and coordination within healthcare systems, the findings of this study suggest that excessive reliance on these systems may introduce new forms of vulnerability that are not captured by conventional performance or maturity assessments. A central insight of this research is that digital saturation emerges not from the mere presence of digital systems, but from an imbalance across the core dimensions of the Stability–Efficiency–Adaptability (SEA) model. The results indicate that many of the identified risk factors such as high dependency on digital systems, loss of manual alternatives, infrastructure fragility, and system interoperability challenges are not isolated technical issues, but interconnected manifestations of reduced stability and adaptability in the context of increasing efficiency-driven digital integration.

This interpretation highlights a critical limitation of existing digital health evaluation approaches, which often emphasize adoption, coverage, and performance optimization, while overlooking the systemic risks associated with over-integration. In contrast, the SEA-based framework developed in this study provides a more balanced perspective by explicitly capturing the trade-offs between efficiency gains and the erosion of resilience capacities. In this sense, digital saturation can be understood as a systemic condition in which efficiency is maximized at the expense of stability and adaptability, leading to increased fragility and susceptibility to disruption.

The introduction of the Digital Saturation Index (DSI) represents a key methodological advancement. By translating qualitative disruption mechanisms into a structured and quantifiable measure, the DSI enables healthcare organizations to move beyond descriptive assessments toward systematic evaluation of digital system vulnerability. Importantly, the use of SEA-based sub-indices allows for more granular diagnosis, enabling decision-makers to identify whether digital saturation is primarily driven by instability, excessive efficiency orientation, or lack of adaptability. This diagnostic capability enhances the practical utility of the tool, particularly for policymakers and healthcare managers responsible for system design and risk management.

From a practical perspective, the findings underscore the importance of rebalancing digital transformation strategies. Rather than focusing solely on efficiency and automation, healthcare systems should prioritize the development of redundancy, reversibility, and preparedness mechanisms. This includes maintaining functional non-digital alternatives, strengthening infrastructure resilience, ensuring interoperability robustness, and improving user trust and system usability. The observed tendency of users to bypass digital systems further reinforces the need to align technological design with real-world operational practices, as behavioral responses may serve as early indicators of systemic stress and digital saturation.

At the policy level, the proposed checklist and DSI provide a scalable tool for monitoring and evaluating digital system risk across healthcare organizations. By offering a standardized yet flexible assessment framework, the tool can support benchmarking, risk stratification, and targeted intervention planning. This is particularly relevant in contexts where rapid digitalization is being pursued without sufficient consideration of long-term system resilience.

Despite these contributions, several limitations should be acknowledged. First, the checklist and index were developed based on expert consensus and conceptual mapping, and their empirical validation in real-world healthcare settings remains an important next step. Second, the current study applies equal weighting across SEA dimensions to ensure simplicity and interpretability; however, the underlying conceptual framework suggests that the influence of these dimensions may be asymmetric. Future research may therefore explore alternative weighting schemes or non-linear models to better capture the dynamic interactions between efficiency, stability, and adaptability.

In addition, while the current instrument focuses on system-level assessment, further refinement may be required to adapt the tool for different organizational contexts, such as hospitals, primary care settings, or national health systems. Longitudinal application of the DSI may also provide valuable insights into how digital saturation evolves over time and how it relates to system performance and failure events.

In conclusion, this study advances both the conceptual and methodological understanding of digital transformation in healthcare by reframing it through the lens of system balance and vulnerability. By introducing a SEA-based checklist and the Digital Saturation Index, the research provides a practical and theoretically grounded approach for assessing and managing the risks associated with digital over-dependence. The findings highlight the need for a more balanced and resilience-oriented approach to digital health system design, ensuring that gains in efficiency do not come at the cost of system stability and adaptability.

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

1. 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.
2. 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.
3. Bowman, S. (2013). Impact of electronic health record systems on information integrity: Quality and safety implications. *Perspectives in Health Information Management, 10*(Fall).
4. Borycki, E. M., & Kushniruk, A. W. (2023). Health technology, quality and safety in a learning health system. *Healthcare Management Forum, 36*(2), 79–85.
5. 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.
6. 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.
7. Gates, L. G. (2024). Cyber attacks on interoperable electronic health records: A clear and present danger. *Missouri Medicine, 121*(1), 6–9.
8. 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*.
9. Hojabri, R., & Manafi, M. (2025). AI for Health Equity: Bridging the Urban–Rural. *Journal of Creative Perspectives*, *1*(4), 65-71.
10. Hojabri, R., & Manafi, M. (2026a). An Early Warning Framework for Healthcare System Collapse. Journal of Saturation Studies, 1(1), 20-34.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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*.

16. 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.
17. 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.
18. 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.
19. Manafi M. Orientation note: Saturation, collapse, and the Rosetta Stone Model. Manafi Institute for Saturation Studies. https://manafi-institute. de/Resources. 2025."
20. 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."
21. 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.
22. 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.
23. 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.
24. 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.
25. Tilhou, A. S., Jain, A., & DeLeire, T. (2023). Telehealth expansion, internet speed, and primary care access before and during COVID-19. *JAMA Network Open*.
26. World Health Organization. (2020). Artificial intelligence in health care: Accountability and safety.
27. World Health Organization. (2024). *Addressing future cybersecurity threats in digital health: Report of the technical consultation, Geneva, Switzerland, 12–14 December 2023*.
28. 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).