Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 22 No. 11 (2026) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v22i11.63307

SPECIAL FOCUS PAPER

# The Economic Value of Crisis Communication in Digital Healthcare Emergencies: Spokesperson Structures, Trust, and Information Governance

**Eugen Röttinger** (✉)

Academy of Economics, Svishtov, Bulgaria

eroettinger@roettinger-gruppe.de

**ABSTRACT**

The ability to communicate effectively during an emergency is critical when organizations rely on digital technologies. This study analyzes the economic value of crisis communication in digitally-based healthcare environments and focuses specifically upon: (1) the structural arrangements of spokespeople within organizations; (2) institutional trustworthiness; and (3) governance of data/information. Effective crisis communication is best viewed as an essential aspect of a resilient healthcare system rather than simply as an external function of public relations. Building upon literature in the areas of crisis communication, public administration, health governance, and digital health implementation, this study establishes a theoretical model connecting communication capacity to economic resilience outcomes in healthcare emergencies. This paper develops a conceptual model showing how open communication practices, clearly defined spokesperson roles, and coordinated information governance can support stakeholder confidence and improve decision-making efficiency during digital healthcare emergencies.

**KEYWORDS**

crisis communication, digital healthcare emergencies, hospital resilience, information governance, trust, spokesperson structures, economic resilience

## 1 INTRODUCTION

### 1.1 Background: Digital healthcare emergencies

Hospitals have increased their reliance on digital infrastructures to provide, deliver, and coordinate care. Clinical documentation, patient administration, diagnostic processes, emergency communication, internal communication, medication management, telemedicine, and exchanges of data with outside actors are highly dependent upon digital systems. Digital infrastructures have greatly improved efficiencies and transparency

Röttinger, E. (2026). The Economic Value of Crisis Communication in Digital Healthcare Emergencies: Spokesperson Structures, Trust, and Information Governance. *International Journal of Online and Biomedical Engineering (iJOE)*, 22(11), pp. 8–21. https://doi.org/10.3991/ijoe.v22i11.63307

Article submitted 2026-08-21. Revision uploaded 2026-10-07. Final acceptance 2026-10-09.

© 2026 by the authors of this article. Published under CC-BY.

for many aspects of healthcare [1], [2], [3]. However, they create new vulnerabilities. If digital infrastructures fail or are compromised, hospitals may lose access to critical information, communication channels, or operational control mechanisms [4], [5].

There are several types of digital emergencies that hospitals may experience. Examples include cyber-attacks, ransomware events, failure of hospital information systems, disruption of digital communication systems, issues with data quality, malfunctions of decision support systems or public health emergencies where there is high demand for information and rapid changes in available information [5], [6], [7], [8], [9]. In these cases, hospitals will address not just the medical or technical issue, but also a communication and organizational issue. Therefore, crisis communication is not simply an external public relations function. Crisis communication is part of the operational capacity of hospitals to ensure coordination, legitimacy and confidence from stakeholders during uncertain times [10]. Information will go both internally (hospital employees) and externally (patients, relatives, public authorities, emergency services, media, IT providers, regulators, politicians, etc.) [11]. In a digitally mediated emergency, communication will become a key factor in developing resilience in the hospital's response.

## 1.2 Problem statement: Communication failures as economic risk

Communication failures during digital health emergencies will lead to significant economic consequences. Economic consequences associated with communication breakdowns are not always apparent as direct financial losses. Delayed decisions, duplicate tasks, poor resource use, failure to comply with emergency protocols, reputation damage, and loss of stakeholder trust are all possible [12]. Hospitals require more time for coordination when there is confusion, missing, or conflicting information [10]. Increased operational disruptions and decreased continuity of care are both possible. The economic significance of crisis communication in digital health emergencies is most pronounced due to the reliance of crisis communication on accurate, timely and credible information. Hospital staff may be uncertain whether digital systems can still be used safely. Patients may receive mixed messages regarding available services, while authorities and media may receive ambiguous statements. Such uncertainty can slow down crisis response and increase the overall cost of managing the emergency [11], [13].

The main challenge is, that the roles of the spokespeople are often not well-defined until after a crisis has occurred. It remains uncertain which people have been given permission by hospital management to speak for them. Different people might give messages based upon their personal perspective [14]. Digital emergencies could further degrade the level of trust, make coordination more difficult and decrease effectiveness of the emergency plan [15]. Therefore, communication needs to be seen as more than just an image or a reputation risk, it also plays a part in the economic resilience [12].

## 1.3 Research aim and research question

This study aims to develop a conceptual understanding of how crisis communication contributes to economic resilience in digital healthcare emergencies. In contrast to approaches that treat crisis communication as a reactive activity after operational planning has been completed, this study conceptualizes crisis communication as a proactive capability that supports decision-making, stakeholder coordination, and organizational continuity.

The research question guiding this study is: How can crisis communication contribute to the economic resilience of hospitals during digital healthcare emergencies through clear spokesperson structures, trust-building mechanisms, and effective information governance?

To answer this question, the study pursues the following research objectives:

Research Objective 1: To conceptualize crisis communication as an economic resilience capability in digital healthcare emergencies.

Research Objective 2: To examine how clearly defined spokesperson structures can reduce communication ambiguity and coordination costs during digital healthcare crises.

Research Objective 3: To analyze how trustworthy crisis communication can stabilize stakeholder behavior and support the acceptance of digital response measures.

Research Objective 4: To assess how information governance can improve decision quality, message consistency, accountability, and operational continuity in digital healthcare emergencies.

Based on these objectives, the study develops an integrated conceptual model and derives implications for hospital management and digital health governance.

### 1.4 Contribution and structure of the article

This study advances the current body of research by integrating crisis communication with digital healthcare emergency responses, information governance, and economic resilience. Current research examines the above-mentioned disciplines as independent areas. Crisis communication researchers focus on building trust and credibility while developing stakeholder relationships. Researchers who examine digital health governance have focused on addressing issues related to data, systems and accountability. Resilience within hospitals has been defined through three dimensions: preparedness, continuity and adaptability. Thus, this article will bring these concepts together and argue that communication structures are an important aspect of governance in providing the foundation for resilient hospitals.

The practical contribution of this study includes demonstrating how hospitals can develop communication responsibility definitions, identify spokesperson roles, and design information governance processes prior to experiencing a digital disaster response. While the purpose of crisis communication is to explain a crisis to the public it also serves to help reduce uncertainty and facilitate coordination of decisions in order to protect the operational and financial viability of a healthcare organization.

This remaining parts of the paper are as follows: The next section describes the methodological approach. The results section presents the conceptual findings. The discussion interprets their implications for hospital management and digital health governance. The conclusion summarizes the main argument and outlines directions for future research.

## 2 MATERIALS AND METHODS

### 2.1 Study design

This study is designed as a narrative literature review with structured search elements and a conceptual synthesis. This type of methodology has been selected as the field of study on crisis communication during digital health emergencies

is transdisciplinary. Therefore, relevant studies are found within various fields such as crisis communication, public health, hospital management, digital health governance, cybersecurity, organizational resilience, and health economics.

The objective of the review is not to complete an overall systematic evaluation of available empirical data nor to undertake a quantitative meta-analysis. Rather, this article aims to determine and integrate theoretical mechanisms which demonstrate how crisis communication can contribute to resilient responses from hospitals. The study will not attempt to measure the specific monetary benefits of crisis communication. Instead, it will consider the economic benefit as being the potential contribution that communication capacity may have towards the development of organizational resilience (i.e. decision-making and process efficiencies), preserving stakeholder trust, and reducing disruptions.

This methodology provides an appropriate basis for the development of a conceptual understanding of the relationships between the structural components of spokespeople in crisis situations (trust and information governance) and their respective effects upon organizational resilience during digital health emergency crises.

Furthermore, it also provides a mechanism for deriving practical management implications for hospitals and health authorities.

## 2.2 Search strategy and sources

This study employed an organized search to find data in the scientific literature, although it did so in a manner that was not systematic. The primary search tools used in this search were Google Scholar, PubMed, Scopus, and Web of Science. They were selected due to their coverage of different fields of interest within disciplines that relate to healthcare management, public health, communication studies, information systems, and organizational research. The researcher also reviewed select reports and policy documents produced by various institutions (e.g., WHO; National Health Authorities; Hospital Associations) to gain additional contextual perspective when discussing crises related to digital health emergencies, preparedness for those crises, and health information governance.

The search terms were grouped into four thematic areas. The first group addressed communication-related concepts, including “crisis communication,” “risk communication,” “spokesperson,” “public trust,” and “health communication.” The second group focused on healthcare emergencies, using terms such as “hospital resilience,” “healthcare emergency,” “public health emergency,” and “emergency preparedness.” The third group addressed the digital dimension through terms such as “digital health,” “health information systems,” “cybersecurity,” and “information governance.” The fourth group covered economic and organizational effects, including “economic value,” “organizational resilience,” “decision-making,” “coordination costs,” and “operational continuity.”

## 2.3 Inclusion and exclusion criteria

The criteria for inclusion in the study of sources were that the source must be directly related to one of the four following areas:

1. Healthcare
2. Hospital Management

3. Public Health
4. Digital Healthcare Infrastructure

Also, each included source had to discuss at least one of the six dimensions of digital healthcare infrastructure described above:

1. Communication
2. Trust
3. Governance
4. Resilience
5. Emergency Response
6. Organizational Performance

Priority was given to peer-reviewed journals, academic books, review articles, institutional reports. Recent literature was favored because it reflects the growing importance of digital infrastructures in healthcare. Older foundational contributions were also considered whenever their conceptual theories were important to understand, especially in the fields of crisis communication, trust and organizational resilience.

The exclusion criteria included: Technical cybersecurity aspects, where there is no discussion of communication, governance or organizational implications, clinical studies, which do not address crisis management, hospital responses, or healthcare governance and any other source that does not have an obvious link to either organizational resilience or the healthcare context. Finally, popular science articles, journalistic pieces and unverifiable internet information will be excluded from this analysis unless they are used strictly as background examples, but not as empirical evidence.

## 2.4 Analytical approach

The selected sources were analyzed through a structured thematic synthesis. First, all relevant studies were grouped into three categories of analysis based on the three main themes identified by the authors for their research focus i.e., spokesperson structures, trust/trustworthiness, and information governance. These categories were then utilized to determine how organizations' communication responsibilities are structured, how an organization's credibility and institutional confidence are fostered, and how an organization's information is validated/authorized and distributed during digital healthcare crises.

Second, the studies were also analyzed for recurring mechanisms related to economic resilience (e.g., decision speed, coordination efficiency, operational continuity, stakeholder compliance, technology acceptance, and reputational stability). While these dimensions were not intended to be measured directly as financially quantifiable indicators of economic resilience, they represent possible organizational effects which may assist in reducing the costs associated with crisis management and contribute to enhancing hospital performance relative to resilience.

Together, these two analyses resulted in a conceptual model which illustrates the relationship between a hospital's capacities for crisis communication and its outcomes regarding economic resilience. Specifically, the conceptual model posits that well-structured spokesperson arrangements decrease ambiguity, communication,

that builds trust among stakeholders, helps stabilizing stakeholder behaviors, and good information governance enhances decision quality and consistency of messages. Collectively, these factors provide hospitals with a means to maintain operational integrity during digital healthcare emergencies.

# 3 RESULTS

## 3.1 Crisis communication as an economic resilience capability

In crises caused by digital disruptions in health services, the role of communication has changed from a reactive PR function into a proactive operational capability. Crisis communication in digitally mediated hospital emergencies, does not simply provide external messages, manage media relationships or protect reputation [10], [11], [14]. Communication in such situations directly influences the speed at which shared situational awareness develops, how emergency decisions are communicated and justified to internal and external stakeholders, and whether responses based on digital systems are accepted [13].

Therefore, the economic value of crisis communication is derived primarily through indirectly contributing factors related to operations. Crisis communication does not create direct financial returns for the organization. However, it does decrease uncertainty-induced inefficiencies within crisis response efforts [11], [12]. When communication is timely, consistent and credible, organizations are able to develop consensus among their employees and other stakeholders regarding the course of action much quicker. This leads to less likely scenarios where multiple employees take different courses of action, less time spent coordinating employee activities and fewer disruptions to both clinical and administrative functions due to repeated actions taken by employees [12].

Within digital disruptions in health services, this function is particularly critical since uncertainties surrounding system reliability, availability and security, will result in hospital staff needing to determine if electronic health record access remains available. Can digital communication tools still be utilized? Should a manual fallback procedure be initiated? Has patient data been compromised? [5], [7] Patients and family members also need information about the service availability and treatment continuance. Authorities and media require accurate and timely reports that do not minimize or overstate the severity of the situation [13].

Therefore, the synthesis supports the conclusion that crisis communication capabilities generate economic value by decreasing uncertainty-related inefficiency in crisis response. Faster decision-making, more predictable behavior by all stakeholders involved, greater acceptance of using digital-based response methods, lessened risk of reputational damage and increased ability to continue delivering quality care, represent some of these values.

## 3.2 Spokesperson structures: Reducing ambiguity and coordination costs

The first key mechanism in the synthesis process is that of spokespersons. Digital health emergencies create uncertainty as to whose authority is being used, what messages are approved, and how to integrate medical/technical/administrative/legal perspectives. Defined spokesperson structures will decrease this uncertainty as

they will define responsibility for communicating before such a situation escalates [16], [17].

Hospital leadership or executive spokesperson is needed to give institutional positioning of an organization and make strategic communication. Medical spokesperson is needed to explain clinical implications, patient safety concerns or changes in service delivery. Technical infrastructure spokesperson can clarify hospital information systems, cybersecurity incidents, platform outages or digital workarounds. Liaison functions with public health authorities, emergency services or regulators, are important to align within the hospital. Data protection or information governance representative could be needed if sensitive information were an issue during the situation [17].

If there was no established spokesperson structure, several risks would emerge [14], [16], [17]:

- Different departments may communicate through parallel channels
- Medical staff could put out statements that do not line up with technical assessments
- IT department could speak in a language that is too technical for patients or media
- Hospital management might delay communication until legal issues are clear

All of this can lead to contradictory messages and/or a slower approval process and increase internal confusion. In addition, stakeholders' confidence might be impacted negatively.

A functional spokesperson structure therefore requires more than naming a single media contact. It needs responsibilities, escalation paths, message approval procedures, prepared communication protocols and connections to the operational situation room. The spokesperson system needs to take complex operational information and translate it into coherent messages for different audiences without losing accuracy [16], [17].

The economic relevance of spokesperson structures lies in their ability to reduce coordination costs. If communication responsibilities are clear, less time is spent negotiating who may say what. Decisions can be communicated faster, misinformation is less likely to spread, and the risk of reputational damage decreases. Coordination with authorities, emergency services, IT providers, and other partners also becomes more efficient [12].

**Proposition 1:** Clearly defined spokesperson structures reduce communication ambiguity and thereby lower coordination costs during digital healthcare emergencies.

### 3.3 Trust and trustworthiness: Stabilizing stakeholder behavior

The second mechanism found in the synthesis relates to trust and trustworthiness. Trust is much more than simply an intangible reputational asset for hospitals in times of health crises [18]. Trust impacts how stakeholders react to information, follow orders, collaborate in emergency situations, and tolerate ambiguity. In digital health crises, trust is especially critical because affected stakeholders typically cannot personally evaluate their technical environment. Instead, they rely on the hospital's credibility and its communicators [5], [10], [19].

To have trustworthy communication during a crisis, the hospital needs to present itself as a credible source by presenting information that is competent, truthful,

consistent, timely, and accessible [6], [16], [19]. Competent refers to the ability of the hospital to recognize the crisis and manage the emergency. Truthfulness refers to acknowledging uncertainty, risks, and the limits of available knowledge. Consistent means no representative from the hospital should give contradictory explanations. Timely is referring to communicating early enough before speculations occur and rumors start to form. Accessible is using simple language for the intended audience when you explain complex medical, technical, or legal concepts [6], [16].

The importance of trust is apparent for many stakeholders. Relatives and patients will feel safer knowing that care continues safely, and that management is working on service disruptions. Hospital staff need trust in that there are factual basis of decisions made by leaders; and that they will know what steps they need to take. Public officials need to believe the hospital is providing accurate communication and working together with other external crisis teams. The media, general public, and digital service providers have significant impact on how the overall reputations of the hospital are impacted [11], [13], [14], [18].

In addition to those challenges mentioned above, digital emergencies create additional trust challenges. Stakeholders may question if the data they are receiving is correct and genuine. They may also wonder, whether the digital system failure could be putting patient safety at risk [5], [7]. Therefore, communication must express uncertainty without making it appear as though the institution is losing control. While the hospital may indicate that we do not know some technical specifics, the hospital can say what actions are being taken, which services continue to operate normally, and when next updates will occur [6], [16].

The economic value of trust lies in the stabilization of stakeholder behavior. Trust can increase compliance with emergency procedures, reduce resistance to temporary workarounds, limit rumors and escalation, support the acceptance of digital response measures, and protect institutional reputation. Conversely, loss of trust can increase complaint volumes, media pressure, internal resistance, and post-crisis recovery costs [12], [14], [20].

**Proposition 2:** Trustworthy crisis communication stabilizes stakeholder behavior and supports the acceptance of digital response measures, thereby reducing disruption-related costs.

### 3.4 Information governance: Improving decision quality and communication consistency

The third mechanism identified in the synthesis concerns information governance. While it is true that a great deal of data is required to respond appropriately to a digital healthcare emergency, what really matters is whether information can be verified, analyzed, approved, exchanged and communicated responsibly. Information governance addresses the relationship between data quality, responsibility/accountability, decision-making and communication ability [21], [22], [23].

In this context, several types of governance issues have significant importance. Who has ownership rights to specific information concerning the availability of the systems, the safety of patients, cyber threats, and disruptions to the delivery of service? Is there sufficient reliability to support decisions regarding those areas? Who has the authority to provide information either internally or externally? Are sensitive patient data and technical security information being protected? How frequently does the situation picture need to be updated? Where are the interfaces

located with agencies/authorities, emergency medical services, IT-vendors, Data Protection Officers and media communication teams?

If an organization does not have effective mechanisms for managing their information in crises, they will experience a fractured response. Each unit responding to the crisis will likely use a different version of the situation picture. Leadership in the hospital will get only partial or late information. The communication team may not know how to differentiate fact from assumption. If data protection is overly restrictive it could delay needed updates. Technical experts may withhold information based on confusion over communication responsibilities. All of these failures lead to conflicting messages, delayed responses, increased privacy risk, lack of clear accountability, and inconsistent communication to all stakeholders [22].

Information governance provides a strong foundation for resilient response through providing well-defined routes between data, decision-making and communication [21]. It allows organizations to develop consistent messaging, accelerate assessments of the situation, improve resource deployment, enables legally compliant communication and increases transparency surrounding priority-setting. An example of this would occur when a hospital's information system fails. Governance structures would outline how the status of recovery for the failed system is determined, activate manual procedures as needed, define who informs clinical departments, inform patients and determine what level of disclosure of information can be made available to external stakeholders [5].

The economic connection is evident in several ways. Better data quality reduces the likelihood of wrong decisions. Clear approval processes shorten response times. Data protection and compliance structures reduce legal and reputational risks. Interoperable information flows improve coordination with external partners. Transparent information governance also reduces the burden on individual decision-makers because it creates predefined routines for handling uncertainty [8], [22].

Information governance therefore acts as a bridge between digital infrastructure and crisis communication. It ensures that communication is not only fast, but also accurate, authorized, and accountable. This is particularly important in healthcare, where communication errors can affect patient safety, regulatory compliance, public trust, and operational continuity at the same time [5].

**Proposition 3:** Effective information governance improves decision quality and message consistency, which strengthens operational continuity and reduces avoidable inefficiencies.

### 3.5 Integrated conceptual model

The findings can be integrated into a conceptual model of crisis communication as an economic resilience capability in digital healthcare emergencies. This model illustrates three types of input capacities which have their own distinct mechanisms and thus their own unique economic resilience outputs.

The first input capability is a clearly defined spokesperson structure. It reduces ambiguity by clarifying who communicates on behalf of hospital leadership, medical functions, technical infrastructure, public health liaison structures, and information governance. The second input capability is trust-building communication. It stabilizes stakeholder behavior by providing competent, honest, consistent, timely, and understandable information. The third input capability is effective information governance. It improves the reliability, authorization, and consistency of information used for crisis decisions and stakeholder communication.

The conceptual model (see Figure 1 for summary) therefore shows that the economic value of crisis communication is not limited to reputational protection. It lies in the ability of communication structures to stabilize the organization under conditions of digital uncertainty. Crisis communication creates value when it enables hospitals to interpret information faster, coordinate decisions more reliably, maintain stakeholder confidence, and limit avoidable disruption.

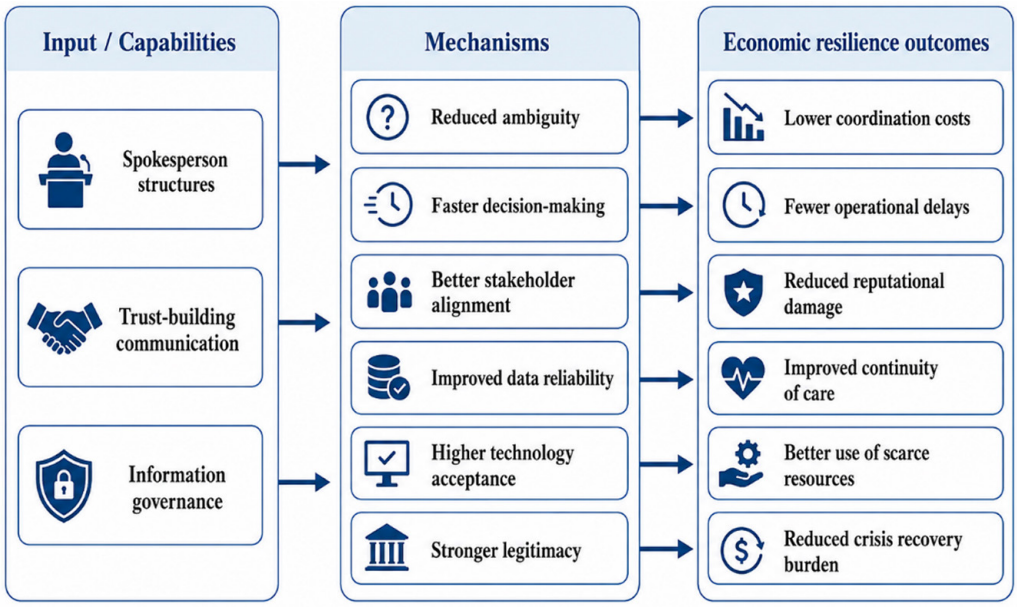



**Fig. 1.** Conceptual model of crisis communication as an economic resilience capability in digital healthcare emergencies

# 4 DISCUSSION

## 4.1 Interpretation of findings

The findings indicate that crisis communication in digital healthcare emergencies should be viewed as an integral part of organizational resilience infrastructure. Crisis communication is not just about providing information to stakeholders once decisions have already been made. As a managerial competency, crisis communication affects how rapidly hospitals develop a common understanding of the crisis; how crisis related decisions are coordinated and legitimized; and how both internal and external stakeholders respond when faced with uncertainty.

Therefore, the strategic economic value of crisis communication arises indirectly from the mitigation of operational uncertainty, coordination costs, delays, reputational risks, and avoidable inefficiencies. This would allow for communication capabilities to contribute to economic resilience by supporting hospitals' continued operation and maintaining stakeholder confidence during disruptions.

In addition, the relationship between crisis communication and economic resilience is significant in digital healthcare emergency scenarios. Cyber-attacks, failure of hospital information systems, loss of digital communication channels, and issues surrounding data quality: they all produce high levels of overlapping risk regarding operational performance, technology, law, and reputation. Additionally, in such environments, crisis communication, trust, and information governance

are highly interconnected. Trustworthy crisis communication requires trustworthy information. Reliable information requires governance structures that provide clear authority. Equally effective Spokesperson structures require that there exist authoritative situational information and decision-making processes.

Thus, the study supports a larger understanding of crisis communication. Crisis communication is not simply delivering messages or protecting one's reputation. Crisis communication acts as a coordinating mechanism, a legitimacy mechanism, and a governance mechanism. By acting as such mechanisms, crisis communication is a critical component of the resilient responses provided by hospitals.

## 4.2 Implications for hospital management

The results show that for hospitals to effectively manage crises, they need to embed their crisis communication plans in their emergency preparedness before the occurrence of an online crisis. As a result, it is essential for hospitals to clearly outline all of the roles of public spokespeople, identify the appropriate levels of escalation and the required approvals, as well as develop communication linkages among the hospital's crisis management team(s), the clinical leadership, IT, legal/compliance departments and external authorities. The hospital's communication protocols should address common types of digital crises (such as cyber-attacks on the hospital's systems, failure of the hospital's information technology systems, breach of patients' confidential medical information, interruptions in services provided by the hospital) and provide backup procedural steps that can be manually executed if electronic processes fail. Communication training and simulation exercises should also emphasize communication skills in addition to other technical recoveries/clinical responses.

## 4.3 Implications for information governance and digital health governance

The results of this study indicate there must be a formal relationship for crisis communication to information governance in digital healthcare emergency situations. Data protection, IT security, medical leadership, hospital administration and communication teams cannot function as separate entities during digital healthcare emergency situations. Governance structures should establish the data that is permissible to disseminate, who is responsible for validating the information provided, who will assess technical/clinical risk assessments, and what person(s) are responsible for allowing both internal and external statements. These types of governance frameworks provide a means for hospitals to communicate quickly while providing accountability, data protection and consistent messages.

## 4.4 Limitations and future research

The study was limited to an initial narrative literature review utilizing structured search methods. It did not evaluate systematically the available body of literature (primary empirical data) nor performed a monetary cost/benefit analysis. Thus, future research should test the model using empirical studies via case studies as well as interviewing hospital and crisis communication stakeholders in order to

develop metrics that will measure the economic benefit of having developed crisis communication capabilities.

## 5 CONCLUSION

Digital healthcare emergencies are not only technical or medical crises; they are also communication and governance crises. A cyber-attack, failure of a hospital's information system, disruption of digital communications channels, poor quality of data, or digital public health emergency creates uncertainty for stakeholders within the clinical, technical, administrative, and outside environments of the hospital. During an emergency digital healthcare crisis, the hospital will need to recover its systems, maintain its clinical service delivery, clarify what is known and unknown, which entity is accountable for what, and how those entities make decisions.

This article demonstrated that the economic value of crisis communication was not from the direct monetary return on investment. It emerges from reducing uncertainty, delay, miscoordinated responses, lack of trust in the institutions' responses, and un-necessary disruptions. Crisis communication can improve the speed of decision-making, enable operations to continue with fewer disruptions, reduce the cost of coordination among all parties involved, increase the level of trust and confidence with stakeholders, and protect organizational legitimacy. Therefore, this study supports the notion that crisis communication enhances economic resilience in hospitals by creating stability to respond to digital uncertainties.

The conceptual model presented in this article indicates that a structured set of spokespersons, trust building communication, and effective information governance provides a framework for understanding each other as complementary tools. Defining roles clearly reduces ambiguity on who is permitted to speak; trustworthy communication builds trust and facilitates compliance; information governance provides better quality data and consistent messaging with accountability. These three elements together facilitate maintaining relationships of coordination, legitimacy, and continuity of care while responding to digital emergencies.

Therefore, hospitals need to view crisis communication as a proactive and long-term strategic resilience investment instead of viewing it as a short-term public relations activity. Hospitals should develop formal structures for their communication functions, govern them formally before a crisis develops. Formal development of crisis communication functions allows hospitals to be more prepared to communicate effectively during a digital crisis.

## 6 REFERENCES

[1] WHO, *Global Strategy on Digital Health 2020–2025*, 1st ed. Geneva, Switzerland: World Health Organization, 2021.

[2] N. Menachemi and T. H. Collum, "Benefits and drawbacks of electronic health record systems," *Risk Manag. Healthc. Policy*, vol. 4, pp. 47–55, 2011. https://doi.org/10.2147/RMHP.S12985

[3] H. Sikandar, A. F. Abbas, N. Khan, and M. I. Qureshi, "Digital technologies in healthcare: A systematic review and bibliometric analysis," *Int. J. Onl. Eng.*, vol. 18, no. 8, pp. 34–48, 2022. https://doi.org/10.3991/ijoe.v18i08.31961

[4] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," *J. Med. Internet Res.*, vol. 20, no. 5, Art. no. e10059, 2018. https://doi.org/10.2196/10059

[5] E. Larsen, D. Hoffman, C. Rivera, B. M. Kleiner, C. Wernz, and R. M. Ratwani, "Continuing patient care during electronic health record downtime," *Appl. Clin. Inform.*, vol. 10, no. 3, pp. 495–504, 2019. https://doi.org/10.1055/s-0039-1692678

[6] WHO, "Communicating risk in public health emergencies: A WHO guideline for emergency risk communication (ERC) policy and practice," World Health Organization, Geneva, Switzerland, 2017.

[7] H. T. Neprash *et al.*, "Trends in ransomware attacks on us hospitals, clinics, and other health care delivery organizations, 2016–2021," *JAMA Health Forum*, vol. 3, no. 12, Art. no. e224873, 2022. https://doi.org/10.1001/jamahealthforum.2022.4873

[8] N. G. Weiskopf and C. Weng, "Methods and dimensions of electronic health record data quality assessment: Enabling reuse for clinical research," *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 144–151, 2013. https://doi.org/10.1136/amiajnl-2011-000681

[9] A. Wright *et al.*, "Analysis of clinical decision support system malfunctions: A case series and survey," *Journal of the American Medical Informatics Association*, vol. 23, no. 6, pp. 1068–1076, 2016. https://doi.org/10.1093/jamia/ocw005

[10] B. Reynolds and M. W. Seeger, "Crisis and emergency risk communication as an integrative model," *Journal of Health Communication*, vol. 10, no. 1, pp. 43–55, 2005. https://doi.org/10.1080/10810730590904571

[11] T. C. Hayirli, N. Stark, J. Hardy, C. R. Peabody, and M. J. Kerrissey, "Centralization and democratization: Managing crisis communication in health care delivery," *Health Care Manage. Rev.*, vol. 48, no. 4, pp. 292–300, 2023. https://doi.org/10.1097/HMR.0000000000000377

[12] R. Agarwal, D. Z. Sands, and J. D. Schneider, "Quantifying the economic impact of communication inefficiencies in U.S. hospitals," *Journal of Healthcare Management*, vol. 55, no. 4, pp. 265–282, 2010. https://doi.org/10.1097/00115514-201007000-00007

[13] L. M. Ow Yong, X. Xin, J. M. L. Wee, R. Poopalalingam, K. Y. C. Kwek, and J. Thumboo, "Perception survey of crisis and emergency risk communication in an acute hospital in the management of COVID-19 pandemic in Singapore," *BMC Public Health*, vol. 20, no. 1, p. 1919, 2020. https://doi.org/10.21203/rs.3.rs-23558/v2

[14] W. T. Coombs, *Ongoing Crisis Communication: Planning, Managing, and Responding.* Sixth edition. Los Angeles, CA, USA: SAGE Publications, 2023.

[15] L. S. Van Boven *et al.*, "Hacking acute care: A Qualitative study on the health care impacts of ransomware attacks against hospitals," *Annals of Emergency Medicine*, vol. 83, no. 1, pp. 46–56, 2024. https://doi.org/10.1016/j.annemergmed.2023.04.025

[16] Centers for Disease Control and Prevention, "Crisis and emergency risk communication: Spokesperson," Centers for Disease Control and Prevention, Atlanta, GA, USA, 2014. [Online]. Available: https://www.cdc.gov/cerc/media/pdfs/CERC_Spokesperson.pdf

[17] Federal Emergency Management Agency, "ICS organizational structure and elements: Extracted from E/L/G 0300 Intermediate incident command system for expanding incidents," Emergency Management Institute, Emmitsburg, MD, USA, Rep. E/L/G 0300, 2018. [Online]. Available: https://training.fema.gov/emiweb/is/icsresource/assets/ics%20organizational%20structure%20and%20elements.pdf

[18] M. Calnan and R. Rowe, "Researching trust relations in health care: Conceptual and methodological challenges – an introduction," *Journal of Health Organization and Management*, vol. 20, no. 5, pp. 349–358, 2006. https://doi.org/10.1108/14777260610701759

[19] R. G. Peters, V. T. Covello, and D. B. McCallum, "The determinants of trust and credibility in environmental risk communication: An empirical study," *Risk Analysis*, vol. 17, no. 1, pp. 43–54, 1997. https://doi.org/10.1111/j.1539-6924.1997.tb00842.x

[20] M. Siegrist and A. Zingg, "The role of public trust during pandemics: Implications for crisis communication," *European Psychologist*, vol. 19, no. 1, pp. 23–32, 2014. https://doi.org/10.1027/1016-9040/a000169

[21] S. Ghaffari Heshajin, S. Sedghi, S. Panahi, and A. Takian, "A framework for health information governance: A scoping review," *Health Res. Policy Sys.*, vol. 22, no. 1, Art. no. 109, 2024. https://doi.org/10.1186/s12961-024-01193-9

[22] M. R. H. Khan, M. M. Rana, and M. M. Rahman, "ZTX-BAIC: A multi-layered cloud security framework integrating ZTA extended with blockchain, AI, advanced encryption, and CSPM," *International Journal of Online & Biomedical Engineering*, vol. 22, no. 2, pp. 124–141, 2026. https://doi.org/10.3991/ijoe.v22i02.58239

[23] A. Ramirez, R. Pingo, S. Wong-Durand, P. Castañeda, and A. Oñate-Andino, "BioBERT-XGBoost for adverse drug reaction prediction: An interpretable hybrid model for risk-aware pharmacovigilance," *International Journal of Online & Biomedical Engineering*, vol. 22, no. 4. pp. 107–122, 2026. https://doi.org/10.3991/ijoe.v22i04.59703

## 7 AUTHOR

**Eugen Röttinger, M.Sc.** is a doctoral researcher at the D. A. Tsenov Academy of Economics, Svishtov, Bulgaria. His research interests include crisis communication, digital healthcare, organizational resilience, cybersecurity, information governance, and crisis management (E-mail: eroettinger@roettinger-gruppe.de).