DIGITAL TRANSFORMATION IN YEMEN'S HEALTHCARE SECTOR: ENHANCING DATA PROTECTION AND RESILIENCE

J. A. A. Blalah[1], M. F. S. H. Al-Kamali[2]

[1]*Scientific Organization for Research and Innovation, Yemen*

[2]*Sukhoi State Technical University of Gomel, Republic of Belarus*

This works examines technology-based strategies for enhancing data protection and digital resilience in Yemen's healthcare sector amidst ongoing challenges. It emphasizes the importance of secure systems to improve healthcare access and patient trust.

Keywords: data protection, digital resilience, healthcare transformation, Yemen, telemedicine.

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ В СЕКТОРЕ ЗДРАВООХРАНЕНИЯ ЙЕМЕНА: ПОВЫШЕНИЕ ЗАЩИТЫ ДАННЫХ И УСТОЙЧИВОСТИ

Дж. А. А. Блала[1], М. Ф. С. Х. Аль-Камали[2]

[1]*Научная организация исследований и инноваций, Йемен*

[2]*Гомельский государственный технический университет имени П. О. Сухого, Республика Беларусь*

Рассмотрены технологические стратегии повышения защиты данных и цифровой устойчивости в секторе здравоохранения Йемена в условиях сохраняющихся трудностей. Подчеркивается важность безопасных систем для улучшения доступа к медицинской помощи и повышения доверия пациентов.

Ключевые слова: защита данных, цифровая устойчивость, трансформация здравоохранения, Йемен, телемедицина.

As Yemen navigates a complex landscape shaped by ongoing conflict and economic hardships, the digital transformation of its healthcare system has become increasingly essential. The integration of technology in healthcare offers significant opportunities to improve access to medical services and enhance patient outcomes. However, this transition raises critical concerns regarding data protection and privacy. Ensuring the security of sensitive health information is vital for maintaining patient trust and fostering effective healthcare delivery in Yemen. This work explores technology-based strategies aimed at enhancing digital resilience in the Yemeni healthcare sector, with a particular focus on data protection measures that can mitigate risks associated with digital health systems.

The healthcare system in Yemen faces numerous challenges, including limited resources, a fragmented infrastructure, and ongoing conflicts that complicate service delivery. As healthcare providers increasingly adopt digital solutions such as electronic health records (EHRs), telemedicine, and mobile health applications, the need for robust data protection mechanisms becomes critical. Data breaches and unauthorized access to sensitive health information can lead to severe consequences, including compromised patient privacy, loss of trust in healthcare providers, and potential legal repercussions [1].

The unique socio-political context of Yemen necessitates a heightened focus on data security. With a significant portion of the population lacking access to reliable communication networks, the digital divide exacerbates existing inequalities in healthcare access. Implementing effective data protection strategies is essential not only for safeguarding individual privacy but also for ensuring equitable healthcare delivery across diverse communities.

A secure Telecommunications Infrastructure (TI) is foundational for protecting health data

in Yemen. Creating a dedicated network for healthcare providers can facilitate secure communication and data transfer, minimizing the risks associated with using public internet connections. By implementing robust encryption protocols and secure access controls, healthcare organizations can safeguard sensitive information from unauthorized access and cyber threats.

The adoption of Electronic Health Records (EHR) can significantly improve patient care by providing healthcare providers with immediate access to comprehensive medical histories. However, to enhance data protection, EHR systems must be equipped with advanced security features. This includes role-based access control, which ensures that only authorized personnel can access specific patient information. Additionally, regular security audits and updates can help identify vulnerabilities and protect against emerging threats.

Telemedicine has emerged as a vital tool for healthcare delivery in Yemen, particularly in remote areas. To ensure the confidentiality of patient consultations, telemedicine platforms must incorporate end-to-end encryption and secure authentication methods. Implementing two-factor authentication can further enhance security by requiring users to verify their identity through multiple channels before accessing sensitive information.

Training and Awareness error remains one of the most significant risks to data security. Conducting regular training and awareness programs for healthcare professionals can help mitigate this risk. By educating staff about best practices for data protection, including recognizing phishing attempts and securely handling patient information, healthcare organizations can foster a culture of security that prioritizes the protection of sensitive health data.

The digital transformation of healthcare is a vital development as societies transition to a post-industrial, knowledge-driven economy characterized by significant advancements in information technology. Effectively integrating new technologies within the health ecosystem requires managing cybersecurity and resilience to reduce vulnerabilities and foster sector growth. However, a lack of understanding regarding the key concepts needed for a strategic vision of sustainable digital healthcare transformation persists.

In Yemen, this transformation faces considerable obstacles. Ongoing internal conflicts, frequent power outages, dependence on alternative energy sources, and the absence of a centralized patient database due to security issues impede the capabilities necessary for resilient cyber/digital healthcare systems. These include knowledge, resources, risk awareness, partnerships, and supply chains. Consequently, the absence of a strong foundational framework likely leads to poor performance across various metrics, exposing organizations to vulnerabilities often without their awareness.

This situation creates a paradox: sufficient domain knowledge, an understanding of uncertainties, and awareness of risks and opportunities are vital for evaluating an organization’s capacity for digital transformation. Poor performance in these areas hampers the ability to assess the risks linked to emerging digital changes, which is essential for justifying further investment in Yemen's healthcare sector.

The digital transformation of Yemen’s healthcare sector offers both opportunities and challenges. As providers increasingly adopt technology to improve services, the significance of data protection becomes paramount. By implementing strategies such as secure telecommunications infrastructure, enhanced EHR systems, robust telemedicine platforms, staff training, collaboration with cybersecurity experts, and data anonymization techniques, Yemen can strengthen digital resilience in its healthcare system. These initiatives will safeguard sensitive health information, build patient trust, and ensure equitable access to healthcare services across the nation.

References

1. Jawad L. A. Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. Abhigyan, 2024, no. 42 (1), pp. 23–31. DOI org/10.1177/09702385241233073 (Original work published 2024)

PRIVACY AND DATA PROTECTION IN DIGITAL HEALTHCARE: CHALLENGES AND INNOVATIONS

G. A. K. Saeed, B. B. Osipov

Gomel State Medical University, Republic of Belarus

This work explores the critical challenges of privacy and data protection in the digital transformation of healthcare. It examines the reliance on digital health systems for storing sensitive medical information and the implications for cybersecurity and patient trust. The discussion highlights the importance of secure Telecommunications Infrastructure (TI), effective authentication methods, and compliance with legal standards to safeguard data. Additionally, the work addresses the use of anonymized data for research purposes and the balance between innovation and patient privacy in telemedicine services.

Keywords: privacy, data protection, digital healthcare, telemedicine, cybersecurity, electronic patient records, anonymization.

КОНФИДЕНЦИАЛЬНОСТЬ И ЗАЩИТА ДАННЫХ В ЦИФРОВОМ ЗДРАВООХРАНЕНИИ: ВЫЗОВЫ И ИННОВАЦИИ

Г. А. К. Саид, Б. Б. Осипов

Гомельский государственный медицинский университет, Республика Беларусь

Рассмотрены критически важные проблемы конфиденциальности и защиты данных в условиях цифровой трансформации здравоохранения, а также роль цифровых систем здравоохранения в хранении конфиденциальной медицинской информации и ее влияние на кибербезопасность и доверие пациентов. В ходе обсуждения подчеркивается важность безопасной телекоммуникационной инфраструктур, эффективных методов аутентификации и соблюдения правовых норм для защиты данных. Изложены вопросы использования анонимизированных данных в исследовательских целях и баланс между инновациями и конфиденциальностью пациентов в телемедицинских услугах.

Ключевые слова: конфиденциальность, защита данных, цифровое здравоохранение, телемедицина, кибербезопасность, электронные карты пациентов, анонимизация.

The rapid digital transformation of healthcare has revolutionized the way sensitive medical information is stored and shared. As electronic health systems become increasingly prevalent, ensuring privacy and data protection has emerged as a critical challenge. This work explores the implications of digitization on patient trust, cybersecurity risks, and the necessity for robust infrastructure and regulatory compliance in safeguarding health data. The balance between innovation and privacy is essential for the future of effective healthcare delivery.

As the digital transformation of healthcare accelerates, privacy and data protection have emerged as pivotal concerns. Digital health systems depend on the storage and exchange of vast amounts of sensitive information, including medical records and treatment details, necessitating robust technological infrastructures to safeguard against potential threats.

The digitization of healthcare encompasses various applications, from electronic patient records to telemedicine consultations. These advancements create opportunities for improving healthcare access and efficiency, particularly in high-risk scenarios like