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

pandemics. To this end, secure digital identities, encryption methods, and a reliable telemedicine framework are essential for ensuring data integrity and confidentiality.

However, the increased reliance on telemedicine raises significant cybersecurity concerns and challenges regarding the quality of care. To mitigate these risks, healthcare providers must adhere to industry standards and regulatory requirements, thereby enhancing virtual care processes. This approach not only improves healthcare availability but also contributes to a safer, more efficient system overall.

Data protection ensures that personal information is shielded from misuse and unauthorized access, embodying the principle of self-determination – allowing individuals to control how their data is used. The healthcare sector routinely collects extensive personal data, and it is critical for patients to trust that their medical information remains confidential.

The growing interconnectedness of healthcare institutions necessitates stringent data protection regulations to maintain data privacy during digital transfers and storage. A secure Telecommunications Infrastructure (TI) dedicated to healthcare allows only registered individuals and institutions to communicate and share data safely. Patients can utilize digital services within this framework, such as Electronic Patient Records (ePA) and Electronic Medication Plans (eMP), which enable them to access their medical data and control who has access to it.

In physical settings, identity verification often relies on biometric data or personal identification documents. In digital contexts, secure authentication utilizes usernames, passwords, tokens, or biometric identifiers linked to a person's identity. Participants in the TI, including insured individuals and healthcare professionals, must confirm their identities through electronic health cards or professional cards.

When registering for an ePA, individuals verify their identities using their health cards. Subsequent logins can use alternative methods, such as fingerprints. Each ePA is protected by a unique electronic "file key", ensuring that only authorized individuals can access specific medical documents.

Healthcare providers, including telemedicine services, must comply with legal data protection standards. This includes ensuring that video consultations are conducted using cutting-edge technology with end-to-end encryption to prevent unauthorized access. However, many telemedicine services operate over conventional internet connections, which may expose them to data security vulnerabilities.

Services outside the telecom infrastructure may still face data protection issues, even if they comply with legal standards. For instance, third-party tracking can occur with user consent, leading to data collection for marketing or analytics without the patient's explicit awareness.

The Enhanced Use of Health Data for Research Institutions Act permits the use of data from electronic patient records for research purposes, but only with patient consent and after anonymization to protect individual identities. The Federal Institute for Drugs and Medical Devices (BfArM) facilitates access to anonymized data for research and quality assurance.

While the digital transformation of healthcare offers significant benefits, it also presents critical challenges related to privacy and data protection. Effective strategies must be implemented to safeguard sensitive health information, ensuring both compliance with regulations and the trust of patients in the evolving digital landscape.

The digital transformation of healthcare presents both opportunities and challenges regarding privacy and data protection. Ensuring the security of sensitive health information is paramount to maintaining patient trust and delivering quality care. Robust Telecommunications Infrastructure, effective authentication methods, and adherence to regulatory standards are essential to mitigate cybersecurity risks. Additionally, the

responsible use of anonymized data for research can enhance healthcare outcomes while protecting individual privacy. As the sector continues to evolve, a commitment to safeguarding patient information will be crucial for the sustainable growth of digital healthcare solutions.

References

1. Conduah AK, Ofoe S, Siaw-Marfo D. Data privacy in healthcare: Global challenges and solutions. Digit Health. 2025 Jun 4; 11:20552076251343959. DOI 10.1177/20552076251343959. PMID: 40475296; PMCID: PMC12138216.
2. Jawad L. A. Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. Abhigyan, 2024, no. 42 (1), pp. 23–31. DOI /10.1177/09702385241233073 (Original work published 2024).

БЛОК УПРАВЛЕНИЯ ДЛЯ АВТОМАТИЗИРОВАННОЙ ТЕПЛИЦЫ

М. А. Бабкин, А. Е. Запольский

Гомельский государственный технический университет имени П. О. Сухого, Республика Беларусь

Рассмотрен принцип построения и алгоритм работы блока управления для автоматизированной теплицы на базе микроконтроллера. Описана архитектура системы, включающая сбор данных с датчиков температуры, влажности почвы и воздуха, а также анализ параметров микроклимата, управление исполнительными устройствами, ведение журнала событий и оповещение оператора. Предложен циклический алгоритм работы с обратной связью, направленный на минимизацию влияния человеческого фактора, оптимизацию условий выращивания и повышение стабильности урожайности в режиме реального времени.

Ключевые слова: автоматизированная теплица, микроклимат, микроконтроллер, исполнительные устройства, мониторинг, полив, Atmega 328p, ESP32, управление с обратной связью.

BUILT-IN MONITORING SYSTEM FOR OPERATING MODES OF COMBINED ROAD VEHICLE EQUIPMENT WITH ELECTROHYDROGENATED WORKING BODIES

M. A. Babkin, A. Ya. Zapolski

Sukhoi State Technical University of Gomel, Republic of Belarus

The report discusses the design principle and operating algorithm of a control unit for an automated greenhouse based on a microcontroller. The system architecture is described, including data collection from temperature, soil moisture, and air humidity sensors, analysis of microclimate parameters, control of actuators), as well as event logging and operator notification. A cyclic feedback-based operation algorithm is proposed, aimed at minimizing the human factor, optimizing growing conditions, and increasing yield stability in real time.

Keywords: automated greenhouse, microclimate, microcontroller, actuators, monitoring, irrigation, Atmega 328p, ESP32, feedback control.

Целью работы является создание интеллектуальной системы управления, которая преобразует процесс выращивания растений на уровень высокотехнологичного цифрового производства.

Работа направлена на достижение следующих подцелей: минимизация рисков, оптимизация условий выращивания, повышение урожайности, достижение технологической трансформации.

Минимизация рисков связана с устранением ошибок, вызванных человеческим фактором (забывчивость, несвоевременный полив или проветривание).