Review

INTEGRATED HEALTH INFORMATION SYSTEM IN THE REPUBLIC OF SERBIA

Jasmina Veličković[1], Mitar Lutovac [2], Mia Jokić[3]

[1]Medika College of Vocational Studies in Healthcare, Belgrade, Serbia
[2]Faculty of Business and Industrial Management, Union University "Nikola Tesla" Belgrade, Sremski Karlovci, Serbia
[3]European Business School, Belgrade, Serbia

Received: 28 March 2024**; Revised:** 31 May 2024; **Accepted:** 22 June 2024;
Published: 28 June 2024

DOI: 10.5937/annnur2-50117

Abstract

The Republic of Serbia's integrated health information system (IHIS) serves as a central electronic repository for storing and processing various medical and health-related data. It encompasses patient records, institutional information, details of health interventions and services, electronic prescriptions, appointment scheduling for specialist consultations, diagnostic procedures, and surgical operations. The implementation of this system promises several benefits, including improved access to patient information, expedited diagnostics, enhanced medication selection processes, heightened patient safety measures, more comprehensive health-statistical reporting, and accelerated dissemination of biomedical knowledge. This paper aims to explore the advantages of employing information technologies in healthcare delivery within health institutions, contrasting it with traditional methods of data collection, analysis, and interpretation, specifically focusing on primary healthcare institutions. Drawing upon current professional and societal perspectives, the paper discusses the conceptual framework and objectives of IHIS, emphasizing the significance of leveraging information technologies in healthcare.

Keywords: health information systems, healthcare, informatics, delivery of healthcare, Serbia

Corresponding Author: Jasmina Veličković, e-mail: jasminav.frad@gmail.com

Introduction

In modern times, large amounts of data are generated daily for business and private purposes. Data is typically stored in digital format by default. Information systems, which encompass the storage, transfer, processing, and provision of data to users upon request, facilitate this digital storage. In essence, these systems house data and furnish information tailored to users' needs. Thus, the current era can be characterized as the era of information systems.

Almost all new information technologies quickly find applications in various information systems, resulting in the regular appearance of information systems for entirely new purposes. An information system comprises data, processes, personnel, physical resources, and information technology, which collectively interact to gather, process, store, and deliver essential information to aid an organization[1].

Information technology (IT) encompasses the integration of computer technology (both hardware and software) with data and telecommunications technology. It constitutes a fundamental component of any information system. Within a healthcare institution, the amalgamation of information systems and information technology includes a diverse array of applications and products catering to various types of users[2].

Medical information systems encompass comprehensive details of nearly all daily activities within healthcare settings, holding significant value in medical, financial, and administrative domains. The recognition of this reality, alongside the substantial support that health funds receive from information systems, has driven the broader adoption of medical information systems over the past decade[3].

Data accuracy is crucial for healthcare facilities, as it ensures comprehensive recording of patient information. This recording is essential for objectively monitoring each patient's health condition and providing doctors with insights into their status, interventions performed, and therapies administered. To acquire this data, it's necessary to record and process all relevant information obtained throughout the treatment process, ensuring easy accessibility for future reference. This data serves to provide the necessary information for making crucial decisions regarding further treatment, ultimately aiming to save the patient's life and preserve vital functions, which is the primary goal of the profession.

Collecting and storing large amounts of data in healthcare settings is practically impossible without modern information technologies. To achieve this, certain information technology standards must be applied. These standards facilitate the exchange and comparison of data, ensure interoperability between systems, and implement robust data protection mechanisms.

Healthcare professionals are increasingly recognizing the advantages and opportunities provided by information systems. As a result, they are becoming more interested in analyzing the vast amount of data generated from daily activities. This analysis aims to uncover answers to numerous questions encountered in everyday situations and to find effective solutions (Figure 1).

The aim of this paper is to explore the benefits of utilizing information technologies in healthcare services within health institutions. It compares these modern methods with conventional approaches to data collection, analysis, and interpretation, with a specific focus on primary healthcare facilities.

Information-Communication Systems in Healthcare Institutions

The implementation of a medical information system enables health institutions and their employees to enhance the quality of health services provided, streamline workload, reduce operational costs, and improve patient satisfaction with the care and services offered[4].

Today, doctors expect a medical information system to provide them with comprehensive medical data related to a patient. Additionally, many seek a pleasant working environment with an efficient and user-friendly interface to support their daily routines. They also value tools for generating statistical reports, predicting disease progression, and other applications categorized as elements of health information systems[5].

The first information systems that dealt with health-related data date back to the 1960s and were developed in the United States of America[6]. Since then, numerous systems have been developed to meet the administrative and medical requirements of healthcare institutions.

The first information systems implemented in clinics were initially developed for recording material costs and billing. In the evolution of medical information systems, the administrative segment, including billing, has always been a primary focus whenever a new country introduces information systems in healthcare. The subsequent development step was the creation of systems for scheduling and verifying doctor appointments[7].

Over time, individual information systems have evolved from 'fee-for-service' systems designed to control the budget of a healthcare facility, to systems that fully automate the process of providing healthcare, and finally to expert systems that actively assist doctors in making decisions and efficiently cover each treatment segment.

Today in Serbia, several health institutions, in cooperation with and under the patronage of the Department of Health and other relevant organizations, are planning to implement or are already using various modules of information systems.

As in other parts of the world, the introduction of information systems in healthcare in our country began with the development of software modules for recording used drugs, materials, and provided services. The Republic Institute for Health Insurance (RIHI) prescribed the report format, which is typically submitted monthly, aiming to justify the materials and medicines used and the health services provided.

Advantages of Information Systems in Healthcare

The utilization of information technologies in contemporary healthcare systems is steadily advancing worldwide. While medical information systems themselves are not novel, their widespread and efficient implementation from a technological standpoint has been a prominent trend over the past decade to fifteen years[8]

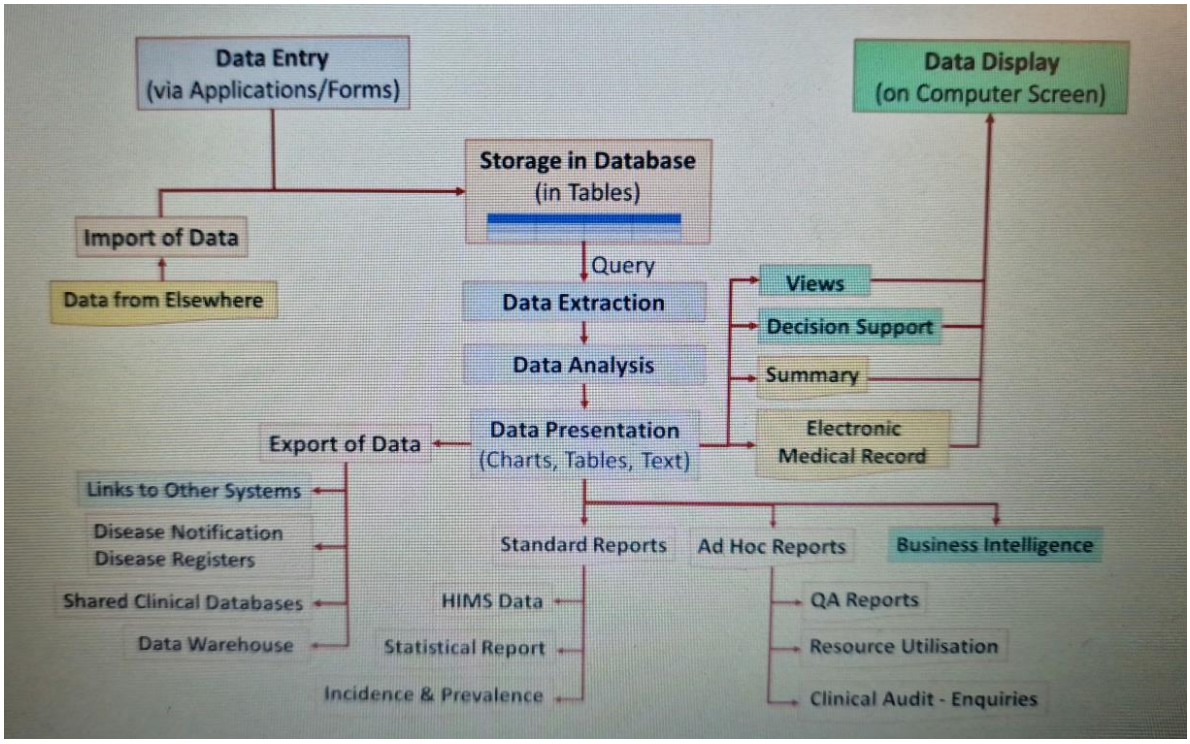

Figure 1. Data flow in the medical information system

Medical information systems play a pivotal role in enhancing the efficiency of healthcare institutions by reducing reliance on paper documentation, maintaining comprehensive records across all aspects of healthcare delivery, and streamlining administrative processes[9]. Moreover, beyond their fundamental function in healthcare, well-designed and effectively implemented systems should also contribute significantly to the advancement of education and research within the field[1].

In accordance with the nature, scope, and complexity of the activity, an adequate information system[3]:

1. Has functionality, capacity, and performance that enable the provision of appropriate support to business processes.
2. Provides timely and accurate information important for decision-making and efficient performance of activities.
3. Is designed with appropriate controls for data validation at the input, during processing, and at the output stages, allowing it to detect inaccuracies and inconsistencies in data and information. To establish and preserve the integrity of the information system, it is necessary to ensure that existing and other data processing systems, as well as the reporting system, are adapted.
4. Provides an appropriate organizational structure with a

clearly defined division of tasks and duties of employees to enable adequate functioning and management of the information system.

5. Adopts and documents an appropriate methodology that establishes all the rules related to the information system.

6. Establishes a risk and security management process for the information system.

7. Has a security policy that governs the principles, methods, and procedures for attaining and sustaining an appropriate level of system and data security. It also outlines the authorization and responsibilities associated with the utilization of information system resources.

The integrated health information system of the Republic of Serbia is structured and designed to facilitate the planning and effective management of the healthcare system, health insurance system, data collection, and processing pertaining to the health status of the population, healthcare financing, and the operational aspects of the health service. The integrated information system of the Republic of Serbia, by law, consists of the following subsystems[10]:

- Health and statistical system.
- Information system of health insurance organizations.
- Information systems of healthcare institutions.
- Information systems of private practice.
- Information systems of other legal entities.

The integrated information system of the Republic of Serbia provides health data to all participants in the healthcare system, with access rights to that data regulated by the participants' rights, roles, and responsibilities.

Numerous entities such as health institutions, insurance funds, pharmaceutical companies, and medical device manufacturers play pivotal roles within the healthcare sector. Effective data exchange among these participants is essential for delivering optimal care to patients, especially during critical moments. Furthermore, the heightened mobility of the population underscores the diminishing relevance of closed medical information systems, which operate in isolation from other systems. Such closed systems often fall short in facilitating seamless information exchange with similar systems, highlighting the necessity for interconnected solutions[3].

The presence of standalone information systems within specific health institutions or limited segments thereof fails to adequately address the ever-expanding requirements for information exchange. Consequently, two imperative processes emerge: integration and collaboration[8].

A prerequisite to enable integration and collaboration is that all medical information systems must meet appropriate standards both in defining and storing data, as well as in facilitating information exchange. The Institute for Public Health of the Republic of Serbia manages data from the Integrated Information System of the Republic of Serbia. It is mandated that the Institute for Public Health promptly notifies the individuals affected by any data security breaches, the Ministry responsible for health affairs, and the Commissioner for Information of Public Importance and Protection of Personal Data.

Every healthcare institution, whether state-run or private, is obligated to implement an information system. This system comprises a technological infrastructure (network, software, and hardware components), organizational structure, personnel, and procedures for collecting, storing, processing, transferring, displaying, and utilizing data and information.

In recent years, the Government of the Republic of Serbia has shown significant commitment to promoting and enhancing the functionality of information and communication systems. This includes the development of an Infrastructure Plan and efforts focused on safeguarding information of special importance.

The statute for the closer arrangement of measures for the protection of information and communication systems of special importance was adopted on November 17, 2016. It provides detailed regulations for protecting these systems[11]. This statute emphasizes the implementation of an organizational structure where roles and responsibilities of employees are clearly defined within the ICT system operator, ensuring effective information security management.

Integrated Health Information System (IHIS)

IHIS (Integrated Health Information System) was introduced in Serbia in 2023 through the Law on Health Documentation and Records[12]. IHIS simplifies the entry, collection, storage, and exchange of data related to the healthcare system in the Republic of Serbia. It features a user-friendly and intuitive interface for seamless data entry and updates. All data is stored and managed within a centralized database.

Furthermore, IHIS is integrated with existing systems used by the Ministry of Health and state-owned health institutions, ensuring interoperability and streamlined operations[13].

The integrated health information system of the Republic of Serbia grants access to health data to all participants within the health system, aligning with their respective rights, roles, and responsibilities.

IHIS of the Republic of Serbia is structured and designed to facilitate the planning and effective management of the healthcare system and health insurance system. Additionally, it serves for the collection and processing of data regarding the health status of the population, healthcare financing, and the operational aspects of the health service. IHIS represents a central electronic system in which all medical and health data are stored and processed. This includes data on[14]:

1. Patients
2. Health workers and associates
3. Health institutions
4. Health interventions and services performed in the HI
5. Electronic instructions and electronic prescriptions
6. Scheduling for specialist examinations, diagnostic procedures and surgical interventions.

Reliable and timely information forms the foundation for decision-making throughout the healthcare system and is crucial for the development and implementation of healthcare policies, legal regulations, healthcare research, human resources development, education, service provision, and healthcare system financing. Given IHIS's diverse user base and comprehensive functionality, its role extends to generating essential information for decision-makers at all levels of the

health system. This includes facilitating evidence-based decision-making by identifying problems and needs within the healthcare sector.

Therefore, according to the World Health Organization, data from various sources serve multiple purposes across different levels of healthcare[15]:

1. Data at the patient level: These data address the healthcare and treatment needs of individual patients, serving as the basis for clinical decision-making. Challenges may arise when healthcare workers are burdened with entering large amounts of data into multiple subsystems due to poor coordination or system integration.

2. Data at the health institution level: This includes data from the institution's busiess and management reports (e.g., drug procurement records), enabling health managers to effectively allocate and manage resources. This involves monitoring stock levels, identifying needs, and guiding procurement decisions.

3. Data at the population level: Such data are crucial for informing public health strategies and decision-making processes. They provide insights into both service users and non-users within the population. High-quality data from all institutions, both public and private, are essential to accurately represent the entire population.

4. Public health surveillance: This integrates information from institutional and community data sources, focusing on identifying health issues promptly to facilitate timely interventions. This includes responses to emergencies, epidemics, and disease outbreaks.

Electronic Medical Record

The basic medical document is the medical record. The medical record is kept for each patient with the chosen doctor. Transient patients do not have an open medical record but are only referred to the protocol number in the Record book. The medical record accompanies the patient throughout his life (Figure 2).

The dental record is defined as the fundamental document for maintaining patient records with a chosen dentist, including dentists specializing in children's and preventive dentistry[16].

The mandatory immunization card is used to record vaccines administered against infectious diseases, in compliance with regulations on population protection against infectious diseases. This card accompanies an individual from birth until the age of 18, which is when the mandatory vaccination program against infectious diseases is fully implemented.

Keeping medical records, creating, and submitting reports constitute fundamental aspects of the work of every health institution (both state and private), health workers, and health associates[17]. The electronic medical record provides a comprehensive view of data from medical documentation stored electronically for each patient. It consolidates all essential health data critical to the patient's long-term health condition, ensuring accessibility during future healthcare provisions. This integration enhances the patient's chances of successful treatment outcomes.

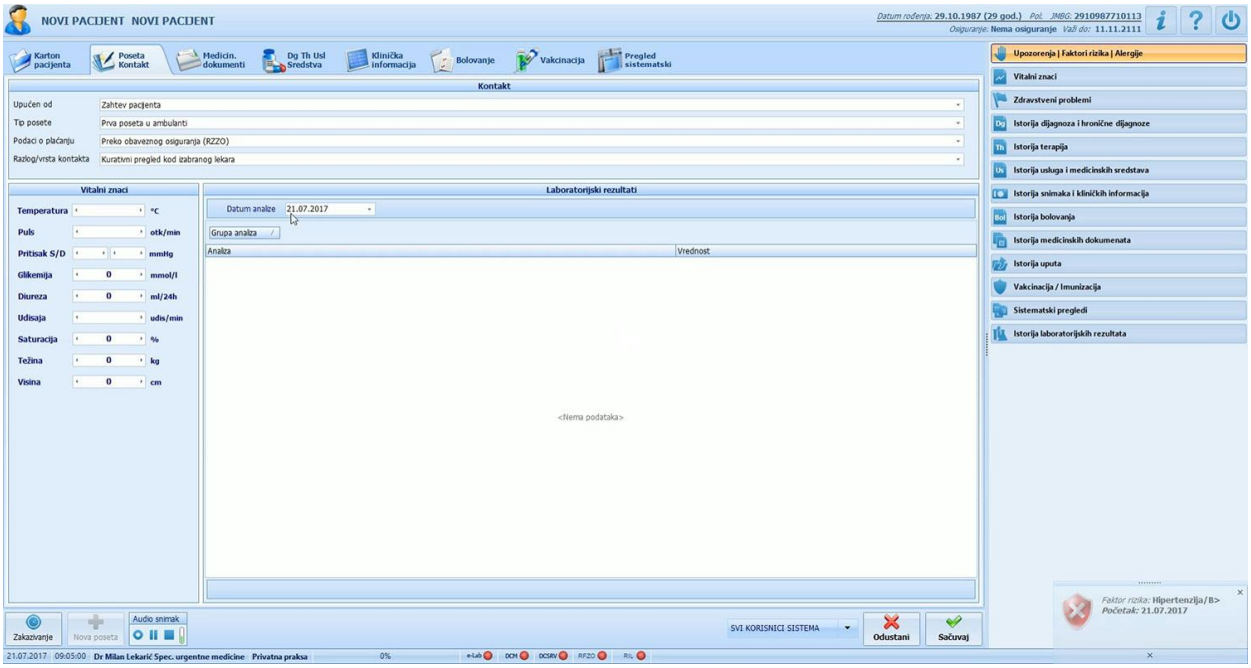

Figure 2. Interface of the electronic medical record

The electronic medical file retrieves medical data from the medical documentation maintained in health institutions (both state and private practices), as well as from the health statistical system and information systems of health insurance organizations[18]. The developed Integrated Information System of the Republic of Serbia serves as the foundation for the introduction of the electronic medical file.

For patients with an electronic health record, medical data is stored electronically. Patients have the right to refuse access to their electronic health record in writing. Patients with an electronic health record are entitled to access their entire medical documentation. If technical requirements are met, patients can also access their medical records online via the Internet (Table 1).

The Personal Data Protection Act governs the collection and processing of medical records[19]. Anyone with access to data is required, while working with medical documentation, to protect it from unauthorized access, inspection, copying, and misuse, regardless of the format in which the medical data is stored (paper, disks, magnetic disks, electronic records such as databases, etc.)[20].

Healthcare institutions, both state and private practices, are required to establish and maintain a security system for medical data in compliance with laws governing the protection of personal data and healthcare documentation. This includes ensuring the integrity of all data recorded in primary medical documentation.

Table 1: Data entered in the basic medical documentation

Patient data	Data on health status and health services
Personal data: surname, first name, surname and first name of one guardian parent, sex, day, month, year and place of birth, marital status, place of residence and stay, JMBG (identification number)	Visitation records
Insurance data	Reason for visit
PNIP (personal number of insured person)	Personal history and objective findings
Chosen doctors data	Diagnosis
Medical data	Health care services provided during stay
Personal medical history	Planned healthcare services
Family medical documents	Refferals to a specialist doctor
Data on disability and incapacity	Referral to hospital treatment
Data on risk factors	Issued medical documents
Social information about patient (level of education, job)	Medication data
Contact details	Issued medical technical aids

The implementation of certified software will facilitate the adoption of electronic health records across all healthcare centers. An electronic health record is a digital representation of an individual's health record, encompassing extensive information about the patient including demographic data, a list of examinations, results of allergy tests, and history of medications or vaccinations. Additionally, it includes receipts for each service or medication utilized by the patient. With the introduction of electronic health records, as soon as a patient registers at the reception desk, the data is automatically transmitted to the doctor's computer, ensuring the doctor has immediate access to the daily schedule and examination plans.

The essential data entered into the EHR system include: demographic information (age, gender, address, marital status, etc.); information on allergies, immunizations, and medical history, encompassing all documents constituting the patient's medical history such as: current status, findings, opinions, list of healthcare providers, results of laboratory tests, radiological findings and images, information on medical treatments, details of prescribed and administered procedures, and medications and materials used.

A health information system serves as the cornerstone for decision-making and encompasses four primary functions: generation, collection, analysis and synthesis, and communication and utilization of information.

The implementation of IHIS has facilitated streamlined and improved planning within the healthcare sector. Its adoption enhances the quality of patient services, transparency of information, and prompt reporting to both patients and the public. Additionally, IHIS promotes an objective approach to patient care, improves accessibility to healthcare institutions, and reduces waiting times for treatment.

ICT Healthcare System Operator

The operator of an ICT system of special importance is obliged, within the organizational structure and considering the nature, scope, and complexity of the business, to determine the duties and responsibilities of employees for managing information security.
The operator of an ICT system determines, within the organizational structure, the tasks and responsibilities of employees for the protection of information assets, i.e., assets and property, for the supervision of business processes important for information security, for risk management in the field of information security, as well as for the tasks specified by procedures in the field of information security[21].

The division of responsibilities among employees should be carried out in such a way as to prevent unauthorized or unintentional modification, damage, or misuse of assets, i.e., information assets, by the operator of the ICT system, as well as to prevent access, modification, or use of assets without authorization and without a record of such actions.

The operator of the ICT system establishes procedures for monitoring activities, auditing, and supervision within the framework of information security management.

When using mobile devices, the protection of data important to the ICT system operator must be ensured, and the risks of using mobile devices in unprotected environments (public places, networks with unknown or insufficient protection, etc.) must be reduced. The ICT system operator considers the following[19]:

1. Records of mobile devices.
2. Physical protection measures for mobile devices (against destruction, damage, loss, or unauthorized access to devices and data important to the ICT system operator).
3. Software installation and update limitations.
4. Installation of adequate software for mobile devices and their regular updating.
5. Limitation of the use of information society services

would threaten the information security of the ICT system.
6. Controls access to the mobile device and the data on it.
7. Cryptographic techniques.
8. Protection against viruses and other malicious software.
9. Remote management of a mobile device in the event of an incident, by an authorized person of the operator of the ICT system, through which it is possible to permanently delete data and prevent further use of the device.
10. Establishment and maintenance of backup data.
11. Enabling safe use of internet services and applications.

Persons who use or manage the ICT system must be qualified for their work and understand their responsibilities. The operator of the ICT system is obliged, by contract or other means, to require employees and other engaged persons not to disclose confidential and other information important for the information security of the ICT system after the termination or change of their employment[21].

Duties and obligations, which remain valid even after the termination of employment, should be included in the terms of the contract with the employee. The operator of the ICT system is obliged to identify and classify the information assets, i.e., funds and resources, through which the creation, processing, storage, transfer, deletion, and destruction of data in the ICT system are carried out. The operator must make an inventory of the information assets, i.e., funds and resources, and establish, maintain, and regularly update their records. Additionally, the operator is obliged to perform classification according to the level of sensitivity and criticality, considering the possible consequences of violating the confidentiality, integrity, and availability of the assets. This classification must be consistently applied, and an adequate level of protection for these assets must be ensured accordingly. For each information asset, i.e., means and property, it is necessary to designate a person responsible for their protection[22].

Data classification must align with the principle of risk management as outlined in the Law on Information Security, ensuring that the level of protection corresponds to the importance of the data[23]. The operator of the ICT system determines the data classification scheme, considering the sensitivity and importance of the data, as well as the potential damage from unauthorized disclosure, modification, or deletion of the data. The operator must apply the regulations governing data protection issues (e.g., classified data, business secrets, personal data, etc.).

The ICT system operator is obliged to define an appropriate set of procedures for handling, processing, storing, and transferring data. When defining procedures and dealing with data carriers, the irreversible deletion of data should be foreseen when the terms for their storage have expired, and they are no longer needed. This includes procedures for approving the removal of data carriers from the premises of the ICT system operator, storing data carriers in a safe place, using cryptographic techniques for data protection as required by regulations, ensuring the safe transfer of data to new data carriers, storing backup copies on separate data carriers, and implementing other measures and procedures for the protection of data carriers[24].

The operator of the ICT system should establish procedures for the safe scrapping and destruction of data carriers when they are no longer needed, minimizing the risk of data access by unauthorized persons. During transport, data carriers should be protected from unauthorized access, misuse, or damage by ensuring reliable transport, utilizing trustworthy personnel, and providing adequate packaging for physical protection. The operator of the ICT system determines which data, in accordance with the data classification scheme, should have records kept of the use of data carriers and the procedures undertaken for the protection of data and data carriers.

Protection of IHIS

The methodology for protecting personal information in medical information systems involves a complex set of strategies including system analysis, risk control, and process control.

The basic steps in developing the methodology for protecting personal information in health institution information systems are as follows:

1. Identification of IT resources requiring protection.
2. Description, i.e., outlining the architecture of the implemented information system and identifying information threats.
3. Assessment of risks in relation to potential damage that may occur.
4. Designing proposals for solutions aimed at reducing risks and mitigating potential consequences.
5. Specification of implemented recommendations[21].

Choosing an adequate protection strategy involves striking a balance between the level and scope of protection, potential risks, and the costs of consequences in case of damage. Health institutions recognize the potential consequences of information confidentiality breaches, underscoring the obligation and necessity for ensuring the safety and protection of personal information throughout the provision of health services[24].

Information security has emerged as a critical factor in the overall development of society, leading to the adoption of numerous standards proven to be best practices in secure information management. The goal of these standards is to secure and protect information and assets from a wide array of threats, whether they are internal or external, accidental or intentional. This is achieved through the systematic introduction, implementation, execution, monitoring, maintenance, and continuous improvement, including upgrades and adaptations to technological advancements in information security systems.

When an organization applies a methodological process to a specific protection project, considering organizational, project, and team dynamics, it is unlikely to perfectly align with any established ICT development methodology. Hence, continuous adaptation, upgrades, and the integration of different methodologies become necessary[24].

In the system, various roles are established to ensure that each user has access to specific functionalities, data, and permissions based on their job responsibilities. Each user in the system is assigned at least one role. Through role assignments, each user logging into the

system is presented with a personalized view and granted access only to functionalities defined according to their assigned roles.

The system has implemented a one-way cryptographic function using hash and salt to securely store user passwords, thereby preventing unauthorized disclosure. To enhance security, passwords must consist of at least 8 alphanumeric characters, including at least one capital letter and one special character. Additionally, the system allows setting a password expiration period. All user passwords are stored securely and cannot be reused. Furthermore, each user is automatically logged out of the system after 15 minutes of inactivity to mitigate security risks.

The service subsystem facilitates integration with other systems through an interface designed for seamless connectivity with existing local information systems used in both public and private healthcare institutions.

Web services are thoroughly documented and accessible through a dedicated web portal for support. Designated users, typically software companies, log in using a username and password to access these resources. Integration is achieved through the implementation of web services, facilitating the exchange of XML documents over HTTPS connections.

Web services can be categorized into two types:

1. **Public Services:** These services do not require authentication and are openly accessible.

2. **Protected Services:** Access to protected services requires user-level authentication. Authentication involves using a username and password obtained from IHIS (Integrated Health Information System). Upon successful authentication, a session token is issued with an expiration time of one hour from the last activity, ensuring secure access to authenticated users only.

An essential component of IHIS is its API portal, which provides detailed documentation of the application programming interface (API). This portal serves to guide the integration of local information systems across primary, secondary, and tertiary levels with IHIS, ensuring seamless interoperability and secure data exchange.

Conclusion

The rapid evolution of ICT has introduced new modes of communication and data exchange that differ fundamentally from traditional systems developed up to that point. To regulate mutual rights and obligations, documents, procedures, and rules have been standardized among participants in the communication process, necessitating skilled professionals, well-organized business processes, and the adoption of modern technologies. Concurrently, alongside ICT advancement, malicious activities by individuals and organizations seeking to undermine these systems have also evolved. To counter such threats, businesses implement comprehensive information security measures to prevent both accidental and intentional disruptions to ICT operations and misuse of information.

Specific measures are defined to protect business information within ICT systems, outlining concrete steps to prevent

unauthorized access to protected information. Continuous efforts are required to safeguard ICT security, aiming to mitigate all forms of risk and elevate ICT protection to an acceptable level.

The implementation of the state medical information system, known as the "Integrated Health Information System of the Republic of Serbia," has centralized medical data encompassing patient records, health personnel details, collaborations, and institutional information. It also includes data on prescribed medications, treatment instructions, and scheduled examinations. This consolidation has greatly facilitated and enhanced planning within the healthcare sector and supported the development of more effective health policies. The system's integration capabilities enable seamless exchange of electronic health records and demographic data with other components of the IHIS of the Republic of Serbia.

Ethical Approval

N/A

Conflict of Interest

The authors declare no conflict of interest.

Literature

1. Protić DD. Information security: Standards or rules. (In Serbian) Vojno delo 2013; 65 (1): 133-150.
2. Wager KA, Lee FW, Glaser JP. Health care information systems: a practical approach for health care management, Fourth Edition. San Francisco CA: Jossey-Bass & Pfeiffer/Wiley, 2017.
3. Janković D, Rajković P, Stanković T, Milenković A, Kocić I. Application of medical information systems in education and research in medicine. Acta Medica Medianae 2012;51(1):73-80. DOI:10.5633/amm.2012.0113s
4. Janković D, Rajković P. Medicinski informacioni sistemi – značaj i struktura. XXXI Simpozijum o operacionim istraživanjima, Iriški venac, Fruška Gora, (2004), 14-17.09.2004; 173-176.
5. Stanković TN, Rajković PJ, Milenković AM, Janković D. User Interface in Medical Information Systems – Common Problems and Sustainable Solutions. Electronics 2010; 14 (2): 59 – 64.
6. Magnuson JA, Dixon BE. (Eds.) Public Health Informatics and Information Systems, 3rd ed. Cham, Switzerland: Springer; 2020.
7. Gostin LO, Turek-Brezina J, Powers M, Kozloff R, Faden R, Steinauer DD. Privacy and Security of Personal Information in a New Health Care System, JAMA 1993; 270 (20): 2487-93.
8. Milenković A. and Janković, D. Primena medicinskih informacionih sistema u Republici Srbiji – trenutno stanje i moguća unapređenja', IT '15, XX Međunarodni stručni skup, Žabljak, Crna Gora, 2015, 23 - 28. Februar 2015, str.. 108-111.

9. Opačić M. Medicinski informacioni sistemi, Informacione tehnologije u medicini, Lekcija 1 (1-13), 2018. https://www.scribd.com/document/411246366/Informacione-Tehnologije-u-Medicini
10. EU-IHIS. Integrisani zdravstveni informacioni sistem'. http://www.eu-ihis.rs /Last access on 22 December 2023.
11. Uredba o bližem uređenju mera zaštite informaciono-komunikacionih sistema od posebnog značaja. Sl. Glasnik RS, 94, 2016.
12. Law on Health Documentation and Health Records. (In Serbian). Sl. Glasnik RS, 92, 2023.
13. Rajković P, Janković D, Milenković A. Developing and deploying medical information systems for Serbian public healthcare: Challenges, lessons learned and guidelines. Comput Sci Inf Syst 2013; 10 (3): 1429–1454. DOI: 10.2298/CSIS120523056R.
14. Janković DS, Milenković A, Stanković T, Marković I, Stojković M, Veljanovski A. Technical Report. Integralni sistem za zakazivanje i obaveštavanje u zdravstvenim ustanovama. Elektronski fakultet Niš - Laboratorija za medicinsku informatiku,2013. http://www.elfak.ni.ac.rs/rs/nauka/projekti/tehnicka-resenja/1287-integralni-sistem-zazakazivanje-i-obavestavanje-u-zdravstvenim-ustanovama.
15. Integrisani zdravstveni informacioni sistem Republike Srbije. https://www.mojdoktor.gov.rs/about
16. Kostić P. Zaštita ličnih informacija u medicinskim informacionim sistemima, Univerzitet Singidunum, Beograd,2004. https://singipedia.singidunum.ac.rs/izdanje/40048-zastita-licnih-informacijau-medicinskim-informacionim-sistemima.
17. Pyne S, Vullikanti AKS, Marathe MV. Big Data Applications in Health Sciences and Epidemiology. In: Handbook of Statistics. Elsevier, vol. 33, 2015, pp. 171– 202. DOI: 10.1016/B978-0-444-63492-4.00008.
18. Marković I, Janković D, Cvetković S. An implementation of electronic dental chart in a medical information system. (In Serbian) INFOTEH-JAHORINA Vol. 9, Ref. E1-7, p. 919-923, March 2010.
19. Zakon o zaštiti podataka o ličnosti. Sl. Glasnik 87/2018.
20. Marković I, Milenković A, Janković D. An Implementation of SMS Communication with Patients in a Medical Information System', ICEST, Veliko Tarnovo, Bulgaria, 2012.
21. Smiljanić N. Elektronska obrada podataka, statistika i administracija, Beogradhttps://iceps.edu.rs/vp-content/uploadsElektronska-obradapodataka-statistika-i-administracija-dr-Smiljanic-Nina.pdf. (2018).

22. Ikić, B.: Organizacija zaštite savremenih informacionih sistema.master rad, Univerzitet Singidunum, Departman za poslediplomske studije, Beograd, 2011. https://singipedia.singidunum.ac.rs/izdanje/41856-organizacija-zastitesavremenih-informacionih-sistem.
23. Janković N. IT kontrola i upravljanje rizicima informacionih sistema, PP prezentacija, INFOTEH 2012., Vrnjačka Banja, (2012) (1-37).
24. Mandić G, Putnik N, Milošević M. Zaštita podataka i socijalni inženjering – pravni, organizacioni i bezbednosni aspekti, Univerzitet u Beogradu, Fakultet bezbednosti, Beograd, 2017.