Overview of current technologies for data protection in healthcare

Miroslav Dechev
Institute of Robotics
Bulgarian Academy of Science
Sofia, Bulgaria
miroslav.dechev@gmail.com

Galya Georgieva-Tsaneva
Institute of Robotics
Bulgarian Academy of Science
Sofia, Bulgaria
galitsneva@abv.bg

***Abstract*— Today's advanced technologies can be used to provide safe and reliable means of sharing personal data in a number of sectors of public life, with their use in healthcare being particularly critical. The large amount of data that is generated daily necessitates the adoption of strict privacy measures. Healthcare is one of the most sensitive areas in this regard, and for this reason there are established regulatory requirements to protect privacy embedded in core standards. The paper examines modern approaches that enable the security and protection of large volumes of health data. Useful tools are presented to improve the privacy of both personal data and research data in the healthcare industry. Advanced digital technologies in implementing patient data protection are reviewed. The research conducted shows that modern protection tools realize effective interactions between healthcare and the patients.**

Keywords — healthcare, data protection, personal data.

I. INTRODUCTION

Digitization in all spheres of our lives has increasingly tied us to electronic devices and the generation of a huge database. However, with the transformation of digital health services and eHealth, technologies to protect patient data are increasingly vulnerable to attacks, unauthorized access and theft. This has put specialists at a huge risk regarding the protection of sensitive medical data. The advancement of digital health infrastructure has brought to the fore modern means of protecting both personal and research data in the health industry, as well as effective interactions between health care and patients.

II. MODERN APPROACHES ENSURING THE SECURITY AND PROTECTION OF LARGE VOLUMES OF HEALTH DATA

A. Overview of working with data in healthcare

Modern technologies overcome time, space, patient access to health services, but pose a risk to the security of personal data. A key feature of digital technologies in the healthcare sector is their flexibility [1].

One of the greatest advantages in modern health care is Internet connectivity, which allows the doctor-patient relationship to be constant over time, without the limitation of physical location. Allows the creation of a patient's medical record with permanent access to treating doctors, medical specialists and administration of health services and institutions. The data in such communication, through modern technologies, is largely defined as sensitive, personal and inviolable and must be protected from unauthorized access by third parties.

On the other hand, depending on the applied treatment or therapy, surgical intervention, hospital or pre-hospital care, devices of different complexity are used, smart technologies, Artificial Intelligence (AI), Virtual Reality, Blockchain, Chatbots, 3D and 4D printing, scanners, nuclear - magnetic resonance imaging (MRI), ultrasound technology, X-ray devices, electronic prescriptions with medications, which contributes to the completion of a huge database of medical data for an individual.

The risk of loss or unauthorized access to consumer medical data also increases exponentially. The integrity of this data is of fundamental importance for the proper and restorative treatment of the patient and it must be ensured technologically.

Using big data to perform macro data analysis enables personalized treatments and helps discover risk factors and potential side effects of drugs [1].

In 2019, the GATEKEEPER [2] project was launched with funding from the EU. The project builds a decentralized digital ecosystem that facilitates collaboration and delivers results to healthcare providers, businesses, entrepreneurs, citizens across Europe. The Information Gatekeeper platform includes over 40,000 patients across nine use cases based on artificial intelligence, eHealth and smart home solutions.

A digital platform that enables these patients to integrate their data into healthcare systems, which will allow better detection of the risks associated with their condition. Likewise, healthcare professionals will have access to real-world data coming from patients and their living environments [2].

The number of patients included in the project in itself speaks for the collection of a huge amount of data that must be protected.

B. Types of approaches in building Information Systems in health care

Today, healthcare authorities pay a lot of attention to ensuring the protection of medical data, because of its importance to the health of the patient and because of the need to protect against unauthorized access (Fig. 1).

ACKNOWLEDGE THE FINANCIAL SUPPORT OF THE PROJECT WITH ADMINISTRATIVE CONTRACT № КР-06-Н57/8 FROM 16.11.2021. - FUNDED BY THE "COMPETITION FOR FUNDING BASIC RESEARCH - 2021." FROM THE RESEARCH SCIENCES FUND, BULGARIA.

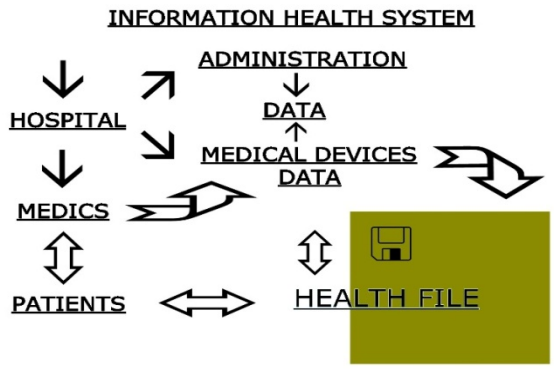

Fig. 1. Information Health System

The main source of medical data in the healthcare system is the electronic health record [3]. Given the transformation of healthcare into a completely new digital environment, the main and key priority is the digital security of personal data, their protection and adequate storage over time.

Digital security is one of the most important aspects of working with clinical information. According to the experts in the field, due to the great granularity of the information and its storage in various repositories of the health structures, it becomes extremely vulnerable to cyber attacks [3].

According to experts and based on serious scientific studies, one of the most important approaches in the collection and storage of medical data is the so-called "unified approach" to the collection and storage of data in a state central repository [3], where all available protection tools are applicable. The introduction of information systems and even more sophisticated devices in health care greatly relieves doctors, sometimes burdened with administrative activities in addition to treatment, and they unwittingly become collectors of a huge amount of data, including: names, ages, diagnoses, results from research, types of therapies, medications. It should be noted that the problem of storing and protecting this huge database requires investment in well-featured and secure hospital information systems.

The technical provision and collection of more information leads to the need to use more and more devices by the medical staff, but with the boom of mobile technology in recent years, this obstacle is significantly easier to overcome [4].

Here, however, one of the biggest challenges arises: the enforcement of information security in hospitals, which stems from the changes in the Health Act and the Personal Data Protection Act, is convinced Eng. Yordan Iliev, head of the Information Department in the "Specialized Hospital for Active Oncology Treatment" (SBALO) [4].

An even narrower and urgent problem is the integration of all this information about the treatment of a given patient, in which case the health facility is defined as the administrator of personal data, the security of which must be ensured. As an important approach in ensuring the security and protection of large volumes of health data, the "integrity" between the individual information systems to which more than one person in the health facility has access stands out.

These are information systems (IS) consisting of multiple modules that are integrated with a common database, and their purpose is to fully cover all business processes in the medical facility - diagnostic activity, inpatient unit, laboratories, farm yard, accounting, finance, human resources, labor and salary (TRZ), and all peripheral support units - TELC, etc., including the provision of services for the patients themselves, for example, access to laboratory results through online checks [4].

The advantages of integrating a core Information System with medical software, for example, are many.

As a good practice, the automation of sending the patient's research data directly to a device for therapeutic procedures is indicated. Thus, the planning data enters the device and it is loaded with the radiation plan and the schedule for conducting the procedures [4]. For example, Radiology Information Systems (RIS) covering imaging devices use global standards, and it is of great importance to integrate them with the patient's file if it is still maintained in another different Information System.

What is specific about RIS is that the medical equipment uses the worldwide standard for transferring and archiving medical image data Digital Imaging and Communications in Medicine - DICOM, including network protocol and file format. The devices also work with the so-called Picture Archiving and Communication System - PACS - image processing and archiving system. PACS processes the images from the devices via DICOM. The connection between the two is extremely important in order to link the patient's data from the registry with the individual systems that are responsible for the different procedures and processes – review, consultation, research [4].

There is a huge risk of loss, error or confusion of medical data if there is no common language - integrated information systems when downloading data from all medical devices, the technological diversity of which is growing at a rapid pace. As an approach to securing health data, it is good risk management already during the construction of the Information System of a medical facility. Approaches in the control of access to health information are at the end of the construction of an integrated information system, are of the most essential importance. Archiving patient information and providing quick access to it through a username and password issued by the medical facility, with the ability to check test results online is also subject to good information protection.

C. Protection of medical data - legal and regulatory requirements

The protection of health data is governed by a number of national and international laws and standards. The main legal acts adopted and in force are:

- GDPR (General Data Protection Regulation) in the European Union: The Personal Data Protection Regulation requires special protection of health information, focusing on informed consent, the right to access and delete data, as well as encryption and anonymization of personal data.

- HIPAA (Health Insurance Portability and Accountability Act) in the US: Regulates the protection of health data and sets rules for the collection, storage, processing and sharing of electronic health records (EHR).

- Legislation in Bulgaria: The Personal Data Protection Act and the Health Act require the protection of personal data, including health information, to be at a high level, taking into account the GDPR rules.

The Health Act [5] introduces an entire section on "Health information and documentation".

According to the normative act, medical and health facilities, RCZ, RIOKOZ, doctors, dentists, pharmacists and other medical specialists, as well as non-medical specialists with higher non-medical education working in the national health care system, collect, process, use and store health information. They are obliged to ensure the protection of the health information stored by them from unauthorized access. According to the provisions of the Health Care Act, as a patient, everyone has the right to the protection of data related to their health status, security and safety of the diagnostic and treatment procedures carried out during their treatment [4].

GDPR and HIPAA regulations set legal frameworks that incentivize healthcare organizations to invest in adequate data protection measures. In most cases, these laws require a high level of security, including data encryption, access control, staff training and regular audits.

Cyber threats easily evolve and become increasingly sophisticated, affecting different industries. Health authorities are the second most targeted industry, ahead of manufacturing. The industry is on alert for a reliable cyber security system [11].

The correct definition of the risks aimed at the organization's information resources includes finding an already existing vulnerability in the built information system and determining the threats to the organization's information resources [6].

It is common practice in developed economies to maintain a so-called "virtual health record" of the patient.

The Virtual Health Record (VHR) (Fig.2) is a collection of individual medical and health records that are located in different information systems and locations on various types of media and under certain conditions become available to certain medical and health experts to inform their management work [7].

The risk to this sensitive information comes from the fact that the medical record very often combines information from many different sources, with the main purpose of tracking an individual's health history.

Despite the numerous benefits of IoT in the healthcare industry, there are security and privacy concerns associated with it. Sensitive personal information is often transferred over an unreliable communication network, making it vulnerable to attacks [12].

An electronic health record is virtual in the sense that the information is not physically located in one place. In addition, voice and video information [7] can be stored, the recordings being formed by many information systems at different times. The initial view of the electronic health record mainly consists of a virtual, computer-based medical record that contains all the information, clinical and administrative and covers all the health and medical experts who have been involved in maintaining the health of a particular individual throughout his life, bringing together all medical specialties, even prenatal and postmortem information, including financial and health insurance services.

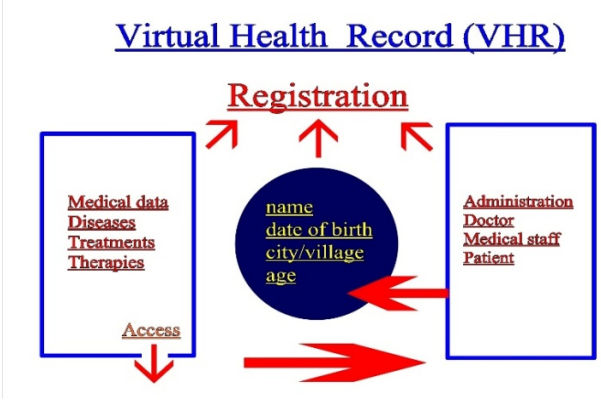

Fig.2. Virtual Health Record (VHR)

III. DEFENSE TECHNIQUES

A. Basic Data Protection Techniques

The architecture for information security must be comprehensive, synchronize all organizational means of control, include comprehensive risk management for information security [6].
The main data protection techniques in healthcare are:

• Encryption

- Data encryption is one of the main techniques for protecting electronic health records when they are stored and transferred between health systems. Encrypting data at storage ensures that even when servers or systems are physically accessed, the data remains unreadable without the corresponding decryption key. Encryption of data in transit is implemented through the use of protocols such as TLS/SSL to protect data when it is sent between medical institutions or external service providers.

• Anonymization

- Anonymization is the process of removing or masking personal identification from health data so that this information cannot be accessed/read by unauthorized persons.
- Pseudonymization is a partial replacement of identifying data, where the original data can be recovered by a certain procedure. This helps protect personal information when analyzing different types of data, results or research, while allowing for tracking when needed.

• Access control

- Access control is implemented through the application of basic principles, methods and systems:

  - Principle of minimum access ("Need to Know"): Each user is granted only the access he needs to fulfill his specific duties. For example, a laboratory technician may only have access to laboratory results, but not to a patient's medical history.

- Role-based access system: In medical information systems, principles of role-based access control (RBAC) are applied, where certain authorized persons (e.g. doctors, nurses, administrative staff) are assigned right of access to certain data, according to their need to handle and access that data. Doctors can access a patient's medical history, test results, diagnoses, etc. Nurses - access to basic patient

information and ability to enter data. Administrative staff - access to personal information (eg insurance details) but not medical records.

- Multi-Factor Authentication (MFA): To increase security, many healthcare institutions implement MFA, which involves combining several levels of security (for example, entering a password/PIN and a phone verification code/token). A form of authentication is also the biometric data of the person (fingerprint, facial recognition, iris recognition, etc.).

- Attribute-Based Access Control (ABAC): Access to data depends on multiple factors (attributes), which may include: User attributes (role, department, rights); data attributes (data type, sensitivity); Contextual factors (location, time, device). For example, doctors can only access a patient's file while they are in the hospital, but not during off-hours or when using an uncertified device.

In the medical sector, contextual information that characterizes an emergency in a patient's health status, for example, must be considered when controlling access to sensitive health information to ensure the most effective treatment. Accordingly, it is necessary to implement access control models that integrate the context concept, such as the idea of dynamically changing contextual attributes that indicate the current status. Specifically, context is considered any information characterizing the status of an entity, such as a person, place, or object, related to the association between an application and a requester [13].

Authentication requires each user to authenticate their identity in order to gain access to the network that is secured. In a number of cases, this is very useful in restricting access to the Internet and its use by authorized users only. Firewalls can be built on the router based on the application layer.

With Network Layer firewalls, the network administrator can set rules in the router to determine access to information through the firewall. In this case, Network Layer firewalls control Internet traffic using access control lists set in the router. These firewalls filter traffic according to the sender address, recipient address, protocol type, and port number of the client that made the request [10].

With these firewalls, the advantage is that larger databases are supported. Application layer firewalls are much more effective in managing the flow of data between internal networks and the Internet, as they check the validity of the data packet, then establish the connection between the client and the server. Application Layer firewalls have proxy servers and application software.

Proxy servers control access to Internet services, and application software configures user authentication, packet filtering, and firewall services. The application software that manages the firewall is also known as a proxy server. One example is the Netscape Proxy Server [10].

• Access tracking

Healthcare institutions use systems to monitor and track data access and operations. Thus, every action (read, write, change or delete) is recorded and can be checked in case of violations or incidents.

• Protection against cyber attacks

Healthcare data can often be the target of cyber-attacks (such as ransomware attacks) due to the high value of medical data that can be illegally sold. Security measures include: Developing anti-virus and anti-malware software; systematic software and operating system updates to minimize vulnerabilities; A data backup (backup) that is secure and independent to restore data in the event of an attack (Fig. 3).

Critical to information security are risk management strategies, security systems testing, and information and network security assessment.

Risk is a combination of the consequences that result from the realization of undesirable events and the probability that these events will occur. Quantitative or qualitative assessment describes risk and allows managers to prioritize risks according to their perceptions of their severity or other established criteria [8].

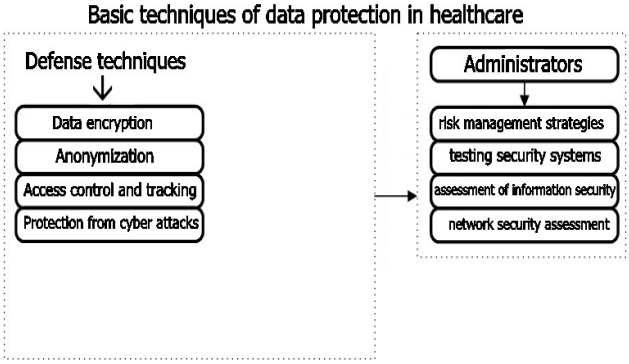

Fig. 3. Basic data protection techniques

Ensuring these protections requires building a security model within an organization. There are several key points to consider in information security policies. Continuous monitoring and analysis of security levels, logging, verification, and activities in information systems provides a high percentage of confidence that the security policy in a system is being properly implemented. Among the safeguards that an organization should pay attention to is the possibility of secure recovery.

Secure recovery ensures that security is not compromised in the event of a system outage or other system failure. Gives rise to two actions: preparing for system failures; system recovery [9].

Another important point when building a system (Fig.4) is the guarantee of its life cycle. It covers control and standardization in the design and operation of a system. Or this is where testing, configuration, verification and deployment come in.

Lifecycle assurance capabilities ensure the planning, development and operation of secure systems under formal and tightly controlled standards. These capabilities are primarily human administrative control [9].

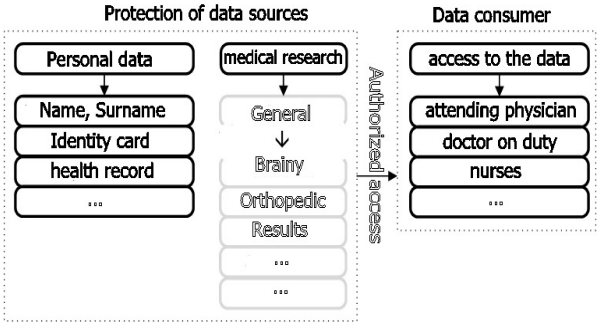

Fig. 4. Sources of medical data

B. *Reasons for the data breach*

The causes of data protection issues in healthcare can be defined as:

- Insufficient training and training of personnel: One of the most serious problems in data protection is the human factor. Many security breaches are due to mistakes or lack of knowledge on the part of medical staff. Ongoing cyber threat education and awareness is needed, as is better password and credential management.
- Protecting mobile devices and telemedicine: With the growth of telemedicine and the use of mobile devices to access medical data, new risks are emerging. Organizations must implement even stricter security policies on these devices, such as encryption, VPNs, and multi-factor authentication.
- Interoperability and data sharing: While the need for interoperability between different healthcare systems is growing, the security of data sharing between organizations often lags behind. There is a need to develop more secure and standardized ways of exchanging data to ensure the security of information during transfer.

With the aim of future desired specialized further processing or copying and reproduction for use in another place, at another time, by other or the same specialists, with the same or new purpose and tasks, the legally regulated rules of storage of medical, hospital, health information should be provided for and rights of access to it [7], as well as its use as evidence in legal, medical processes for example. Traffic filtering, banning the use of devices for which the user is not authorized [6] .

This includes the security of applications and devices that work with network access and managing their vulnerabilities; the control of information flow.

Users may not realize that in the process of working on the Internet, some of their personal health information is collected and manipulated [7].

In this sense, it is extremely important to provide an option of some kind of signaling at potential risky addresses; provision of comprehensive information; clearly defined consequences for refusing to provide personal data [7]; clearly defined responsibility of administration, doctor and patient.

IV. CONCLUSION

Data protection in healthcare is a critical aspect of modern medical practice, and despite steps being taken to improve it, it remains a challenge. Protection methods introduced thanks to legislative regulations such as GDPR in the EU and HIPAA in the US, as well as the implementation of modern technologies such as encryption, multi-factor authentication and role-based access control systems, are effective. Modern technologies such as cloud services with a high level of encryption, artificial intelligence for threat detection and telemedicine platforms with integrated security offer additional levels of protection. The implementation of identity and access management systems and network segmentation also contribute to the effectiveness of protection.

However, healthcare data remains an attractive target for hackers. Ransomware attacks, unauthorized access to systems and data theft are serious threats that many organizations continue to face. For this reason, it is necessary to continue the activities to improve the data protection mechanisms in healthcare.

ACKNOWLEDGMENT

THE AUTHORS ACKNOWLEDGE THE FINANCIAL SUPPORT OF THE PROJECT WITH ADMINISTRATIVE CONTRACT № KP-06-H57/8 FROM 16.11.2021. "METHODOLOGY FOR DETERMINING THE FUNCTIONAL PARAMETERS OF A MOBILE COLLABORATIVE SERVICE ROBOT ASSISTANT IN HEALTHCARE", FUNDED BY THE "COMPETITION FOR FUNDING BASIC RESEARCH - 2021." FROM THE RESEARCH SCIENCES FUND, BULGARIA.

REFERENCES

1. E. Georgieva, Yordanka Mihailova, Nenko Tsvetkov and Nikolay Nedev, THE ADVANTAGES OF NEW TECHNOLOGIES IN DIGITAL HEALTHCARE, Journal of Medical College - Varna, vol. VI, 2023, issue 1 MU-Varna.
2. Internet of Things in European Healthcare, SHAPING EUROPE'S DIGITAL FUTURE https://digital-strategy.ec.europa.eu/bg/policies/internet-things-european-healthcare
3. Digital Healthcare Transformation, Forbes Insights with DHI Cluster, Partner Program, 26 January 2021, 10:26 https://forbesbulgaria.com/2021/01/26/
4. K. Grigorova, Modern technologies and techniques are changing the face of healthcare, Digitalk Capital, May 10, 2013 https://digitalk.bg/internet/2013/05/10/3474077_suvremennite_tehnologii_i_tehnika_promeniat_oblika_na/
5. Health Law, Collection of Laws - APIS, vol. 9/2004, page 20; book 10/2005, p. 105; book 11/2005, page 189 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://old.mh.government.bg/media/filer_public/2018/02/27/zakon-za-zdraveto.pdf
6. V. Vasilev, Management of information security and confidentiality in healthcare facilities, ECONOMIC ACADEMY "D. A. TSENOV" - SVISHTOV DEPARTMENT OF "BUSINESS INFORMATICS", Svishtov 2021.K. https://www.uni-svishtov.bg/portal/getFile/37/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B5%D1%84%D0%B5%D1%80%D0%B0%D1%82-%D0%B4%D0%BE%D0%BA%D1%82.%D0%92.%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D0%B5%D0%B2.pdf
7. Zh. Vinarova, P. Mihova, The Electronic Healthcare System, TEXTBOOK Electronic Healthcare, 5 CHAPTERS https://ebox.nbu.bg/med13/ne7/New%20folder16.V_Glava%20%20ot%20Elektronno%20zdraveopazvane.pdf
8. Stoyanov, N., Ismailov, O., Tselkov, V., Risk management, testing and evaluation of network and information security. Sofia, 2016
9. Petrov, R., Information protection in computers and networks. Sofia, 2002
10. Toms, J., Georgieva, K., Tools for social networks. Marketing in the age of Web 2.0.Sofia, 2011
11. Tomlinson, E.W.; Abrha, W.D.; Kim, S.D.; Ortega, S.A. Cybersecurity Access Control: Framework Analysis in a Healthcare Institution. *J. Cybersecur. Priv.* **2024**, *4*, 762-776. https://doi.org/10.3390/jcp4030035
12. Khan, M.A.; Ullah, S.; Ahmad, T.; Jawad, K.; Buriro, A. Enhancing Security and Privacy in Healthcare Systems Using a Lightweight RFID Protocol. *Sensors* **2023**, *23*, 5518. https://doi.org/10.3390/s23125518
13. Psarra, E.; Apostolou, D.; Verginadis, Y.; Patiniotakis, I.; Mentzas, G. Context-Based, Predictive Access Control to Electronic Health Records. *Electronics* **2022**, *11*, 3040. https://doi.org/10.3390/electronics11193040